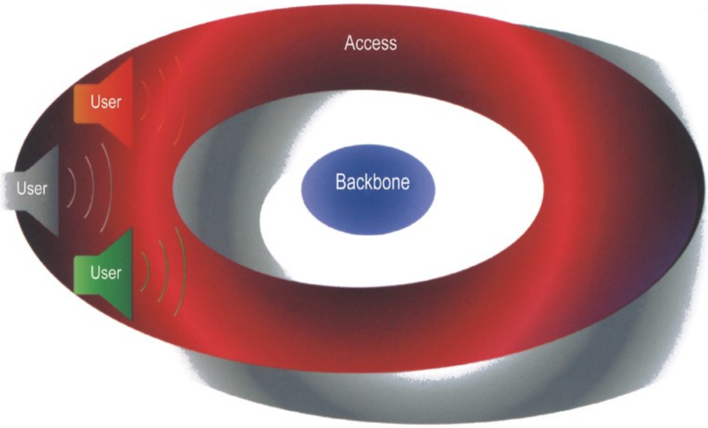
Networking Infrastructure for Pervasive Computing

ENABLING TECHNOLOGIES AND SYSTEMS



Debashis Saha
Amitava Mukherjee
Somprakash Bandyopadhyay

Springer Science+Business Media, LLC

NETWORKING INFRASTRUCTURE FOR PERVASIVE COMPUTING

Enabling Technologies & Systems

NETWORKING INFRASTRUCTURE FOR PERVASIVE COMPUTING

Enabling Technologies & Systems

by

Debashis Saha
Indian Institute of Management Calcutta (IIM-C), India

Amitava Mukherjee
PwC Consulting
Calcutta, India

Somprakash Bandyopadhyay
Indian Institute of Management Calcutta (IIM-C), India

KLUWER ACADEMIC PUBLISHERS
Boston / Dordrecht / London

Distributors for North, Central and South America:
Kluwer Academic Publishers
101 Philip Drive
Assinippi Park
Norwell, Massachusetts 02061 USA
Telephone (781) 871-6600
Fax (781) 681-9045
E-Mail: kluwer@wkap.com

Distributors for all other countries:
Kluwer Academic Publishers Group
Post Office Box 322
3300 AH Dordrecht, THE NETHERLANDS
Telephone 31 78 6576 000
Fax 31 78 6576 254
E-Mail: services@wkap.nl

Electronic Services < http://www.wkap.nl>

Library of Congress Cataloging-in-Publication Data

ISBN 1-4020-7249-X
Networking Infrastructure for Pervasive Computing:
Enabling Technologies & Systems
Debashis Saha, Amitava Mukherjee, Somprakash Bandyopadhyay

Printed on acid-free paper.

Contents

PART II: ENABLING TECHNOLOGIES

PART III: STANDARDS

PART IV: SUMMARY AND FUTURE

Acknowledgements

Many people contributed considerably, either directly or indirectly, in the preparation of this manuscript. It is therefore justifiable that these individuals be acknowledged. First of all, we are grateful to the authors of the papers, articles, books, RFCs, and other reference materials listed at the end of each chapter. In fact, this book is a humble attempt to gather the different viewpoints of the experts in pervasive computing and in particular pervasive networking. Honestly speaking, they know more about each view than we do. They have published their opinions in various journals and magazines (typically special issues of IEEE Personal Communications, IEEE Network and IEEE Communications Magazine) at different points of time. So we are deeply indebted to them for influencing our views in writing this book. Secondly, we have relied on several Internet public documents in writing certain chapters in this book. The concerned links are provided either in the text itself or in the reference section at the end of the chapters. We have culled through many potential sources and there are many references cited in the book. Instead of placing these references in the back of the book in a bibliography, we have chosen to credit them in the appropriate chapters.

Several other people helped us during the course of writing this book. We would specially like to thank our colleagues at Indian Institute of Management (IIM) Calcutta and PwC Consulting, Calcutta. Special thanks go to Amitabh Ray, Agnimitra Biswas, Reena J Sarkar and Sauti Sen of PwC Consulting, Calcutta and Jaydeep Mukherjee of Cogentech Management Consultants (P) Ltd, Calcutta.

It is with pleasure that we also acknowledge and thank the editorial staff of Kluwer Academic. Our editor at Kluwer Academic, Alex Greene, provided the encouragement and friendly coaxing that we needed at the very

beginning to start work on such an ambitious project and finally to bring it to completion. He was also helpful in numerous other ways, small and big. His assistant, Melissa Sullivan, helped with logistics and with her enthusiasm in giving the prompt reminders before the promised deadlines. Finally, our thanks to the production department of Kluwer Academic for managing with a very tight schedule.

Finally, we come to the most important people, namely our family members. We extend our personal gratitude to them for their support and understanding. They endure it with infinite patience and good grace throughout the entire project.

Debashis Saha

Amitava Mukherjee

Somprakash Bandyopadhyay

Preface

There is little doubt that Pervasive Computing (PervComp) is on the brink of becoming an integral part of the everyday lives of a vast number of people. It has found its way into the everyday fabric of our society. The social consequences of this development are difficult to predict, but the technological trends are in place. Several interesting technological innovations provide the possibility of extending the networking environment to traditionally non-networked devices (e.g., microwave ovens and temperature sensors). The cheap and high-speed wired-cum-wireless infrastructure, combined with low-cost handheld devices, appears likely to translate the technological promise of pervasive computing (*PervComp* in short) into a viable economic reality.

This book is a comprehensive guide to tomorrow's world of PervComp in which users can access and manipulate information from everywhere at every time, i.e., every time/everywhere→ every device → every network → every data. Computing devices and networks are becoming ubiquitous. In this new world, computing will no longer be tethered to desktops: users will become increasingly mobile. As users move across environments, they will desire to remain connected all along so that they can continue to access to a dynamic range of application and software services. They will want to carry with them (logically) their unfinished/scheduled tasks including computing, sensing, communicating, etc. Today's infrastructure for networking and communication does not support this model of PervComp very well. Now a days, if a mobile user wants to use the computing resources of a new environment, he/she has to manually figure out how to be connected first and then to perform a computing task using local resources and/or to migrate his/her computing context from another environment. Such manual operation is unacceptable in a pervasive computing world because it does not scale with the increasing amount of different services, user mobility and resource dynamism.

PervComp defines a paradigm shift from mobile computing by introducing the vision of "pervasiveness" i.e., all-time everywhere access to information, communication, services and computing. There are already a host of players in this "business of the millennium". There is the communication industry, the networking industry, the computing industry, the wireless mobile industry, and the Internet industry. However, the interplay amongst these industries in the marketplace is yet to be figured out.

Assuming that the goal is pervasive computing i.e., to turn the computing omnipresent, the technological advances, that are needed to build a PervComp environment, can be framed into four broad areas: networking, middleware, applications and users. This book is primarily concerned with networking technology because the first problem that must be addressed in realizing PervComp is how to establish the necessary underlying infrastructure, known as Pervasive Networking (PervNet). PervNet infrastructure ties different sets of smart nodes together, allowing them to communicate with one another to provide ubiquitous computing services to users. There are several characteristics of the network environment that provide challenging research issues.

Much has changed in the networking world since the inception of the last decade. Advances in wireless and mobile communication have realized "anywhere anytime" connectivity. Optical networks have increased the bandwidth by several orders of magnitude. The requirement of PervNet will sustain and bolster this networking boom in the current decade too. However, a number of issues must be resolved before PervNet burst into picture. There are many technical obstacles- issues of connectivity, levels of service, performance, and reliability and fairness- that stand between the current state-of-art in networking industry and the sort of PervNet that we believe is possible and desirable. These are the challenges that are the focus of this book. Intuitively, PervNet ought to be global, ubiquitous and heterogeneous, and it must have the potential to support diverse applications. But how is it possible to achieve them? What are the available off-the-shelf technologies that would serve as the building blocks? What kind of software architecture is needed to integrate these building blocks into an effective networking platform? Answering these questions is the primary objective of this book- to describe the existing enabling technologies and then to show how these systems can be used to construct a PervNet from the present state.

This book is a uniquely comprehensive study of the major networking technologies and systems that will assist in forming the future PervNet. We first describe the technologies that will help create PervNet, explain the

Chapter 1

Pervasive Computing

Pervasive Computing (PervComp) means different things to different people. For some, pervasive computing is about mobile data access and the mechanisms needed to support a community of nomadic users. For others, the emphasis is on "smart" or "active" spaces, context awareness, and the way people use devices to interact with the environment. And still, others maintain a device-centric view, focusing on how best to deploy new functions on a device, exploiting its interface modalities for a specific task. But, truly speaking, PervComp encompasses all of these areas; it is "*a new way of thinking about computers in the world, one that takes into account the natural human environment and allows the computers themselves to vanish into the background*" as aptly visioned by Mark Weiser of Xerox PARC in his seminal paper [1], [3] published more than a decade ago (1991). That he was much ahead of his time is now widely acclaimed because the current PervComp vision is very much in line with his realization: "*The most profound technologies are those that disappear. They weave themselves into the fabric of everyday life until they are indistinguishable from it.*" So much so that, after a decade, M. Satyanarayan of CMU begins his classical paper [2] on PervComp in 2001 with a quotation of the above two legendary lines of Weiser's article. Incidentally, the stress of both the papers is on those "*machines that fit the human environment, instead of forcing humans to enter their*" because the ultimate goal of PervComp is to "*make using computer as refreshing as taking a walk in the woods*" [1]. So, at its core, PervComp is about four things: users, applications, middlewares, and networks. First, it concerns the way people view mobile/static computing and/or communication devices, and use them within their environments to perform tasks. Second, it concerns the way applications are created and deployed to enable such tasks to be performed.

Third, it concerns the environment, which comprises interface between the applications and the network. Fourth, it concerns the underlying network that supports pervasiveness.

In the vision of PervComp [2], the environment is saturated with a host of computing and communication capabilities which are gracefully integrated with daily life so that user will be able to exchange information and control their environments from everywhere using a seemingly invisible infrastructure of various wireline and/or wireless networks and computing devices. In this introductory chapter, we suggest requirements that this infrastructure must meet to become a "*technology that disappears*", vis-a-vis the shortcomings of the currently existing architectures. While doing so, this chapter also describes the current research in each of the component areas of PervComp, highlighting some common requirements for the intelligent environment of PervComp. Since this chapter raises many questions, few of which are answered by the researchers thus far, the chapter might be regarded as a formulation of research agenda for PervComp too.

1.1. EVOLUTION

PervComp defines a major evolutionary step in a line of work that began in the mid-seventies of twentieth century, when Personal Computers (PCs) burst into the scene of computing. In between personal and pervasive, there are three more distinct evolutionary steps in computing, namely distributed, Web, and mobile [2], all of which have contributed their bits to this evolution. There are some commonalities in the technical problems faced by each of them, resulting into a priori knowledge base for some of the challenges of PervComp. However, there are a host of problems unique to PervComp for which no mapping to knowledge base exists. This book will cover both the categories of problems from networking perspective mainly.

1.1.1 Personal Computing

PC revolution was the first step in bringing computers closer to people; but the idea of making a computer personal was technologically misplaced [1]. This is why, even after thirty years, PC is visibly distinguishable from our daily life, apart from its complex user interface problem which forces people to learn complex jargons quite different from the tasks for which they use PCs. Although, from users' perspective, it was unable to deliver the real potential of information technology, it was certainly the first step towards making computers (may not be computing) popular (may not be pervasive). It was also instrumental behind the phenomenal growth of hardware components and as well the development of graphical user interface (GUI), which are two major components of PervComp. However, the lack of connectivity (computer communication was not known till then) was the major hindrance to information sharing amongst the isolated PCs and that stopped it from being truly global.

1.1.2 Distributed Computing

Personal computing evolved to distributed computing with the advent of networking, in particular LANs and the Internet. Computers started being connected to one another through networks so that data, such as files and emails could be exchanged. Over time, more and more of the computer's capabilities are being shared over the network creating the realm of distributed computing. Distributed computing is simply applying the two old sayings to the realm of computer resources. The first, "Many hands make light work" refers to the idea that you can take a task and break it down so that many different people or computers can work on it at the same time. Then it only takes a small amount of work by each computer (or human) to complete the bigger task. The second saying, "The whole is greater than the sum of its parts" applies to the fact that, when a number of computers work in conjunction, the result is something that cannot be achieved by the computers working alone. One of the benefits that a distributed system has is that it can continue to operate even if some of its parts are missing. This results in much better reliability of the system than a single computer could ever provide.

Distributed computing marks not only the next step in making computers pervasive but also the first step in turning computing pervasive by introducing distributed systems supporting seamless information access, and remote communication with fault tolerance, high availability, and security [2]. Many of these aspects are still pertinent for successful deployment of PervComp, and the corresponding theories, algorithms and frameworks will obviously add to the foundation of the calculus of PervComp. For instance, protocol layering, packet switching, information caching, distributed file and database systems, and encryption techniques will also be needed in PervComp. Surprisingly, no real-life big implementation of distributed computing has been feasible because of immature development of theory. Several attempts to realize a distributed operating system were aborted. It became evident that “strong coupling” and “global distribution” are two contradictory requirements. So the focus shifted to loosely coupled network of networks that can behave as a wide computing platform. However, the biggest drawback of wired distributed computing was its inability to support mobility when motion is an integral part of our everyday life.

1.1.3 Web Computing

World Wide Web (WWW), or simply the Web, which evolved from the Internet, as a computing platform, is probably the only successful implementation of distributed computing in its loose sense. The Web's emergence has fundamentally changed the way many people interact with computers. Though WWW was never designed to be a distributed computing infrastructure, its networking ubiquity has made it an attractive choice for experimenting with distributed computing concepts. It has also created a culture that is substantially more amenable to the deployment of PervComp environments than that which existed when Weiser [1] first articulated his vision. Its ad hoc nature of growth has proved that it is possible to think in such a big way without loosing scalability. Its simple mechanisms for linking resources have showed the way to integrate distributed information bases into a single structure. Most importantly, the Web has pioneered in demonstrating that it is possible to create a nearly ubiquitous information and communications infrastructure. Not surprisingly, the unprecedented success and growth of the Web motivated researchers to investigate the means of combining Web infrastructure with ubiquitous concepts. The Web has had other, more subtle effects on our culture too. First, the increased use of computers as portals to the Web has reduced many users' sense of attachment to a single computing device. Many users now relate not to their computer but rather to their point of presence within the digital world-typically, their homepage, portal, or email service. So, for users who extensively use Web services and information, the computer that they use to access these things has become largely irrelevant. However, WWW is not pervasive into the real world of physical entities, neither was it designed to be. For example, it was not suitable for mobile users (TCP/IP does not support mobility automatically). But it certainly has the potential to serve as a starting point for PervComp because, for most users having access to the same point in digital space from several computers at different places, computers themselves are becoming increasingly unimportant. In this sense, the Web has already made computing somewhat pervasive, and researchers are very quick to understand that (evident by the number of PervComp projects based on web infrastructure [3]).

1.1.4 Mobile Computing

Adding mobility to Web computing has taken us to mobile computing (MobiComp) only recently. The rapid proliferation of mobile devices started with cellular mobile technology such as GSM. Both the size and price are falling everyday, proving Weiser correct in anticipating that, in PervComp, users can use any ubiquitous computing devices, such as ParcTab, as if it were their own. Separating the handset from the subscriber identity module (SIM) card found in GSM systems approximates this model of operation. By inserting their SIM card into a handset, subscribers can automatically use any handset, placing and receiving calls as if it were their own phone. Additionally, modern mobile phones offer far more capabilities than early ParcTabs in roughly the same form factor. A typical phone today might include simple PDA applications, such as a calendar and to-do lists, games, text-messaging facilities, voice communications (of course), Web access, and even simple voice recognition. The convergence of new Internet technologies, such as web application servers, extensible markup language (XML) and Lightweight Directory Access Protocol (LDAP), and mobile technologies, such as the Wireless Application Protocol (WAP), has made it practical to extend wired application information out to mobile user populations. In addition to this revolution in reaching out mobile communication to the masses, technology for mobile wireless networking for voice/data transmission has been obvious for some time (e.g., wireless LANs, ad-hoc networks etc.). We can now access a huge wealth of knowledge and services of the Web from almost any computer, including low-power mobile devices such as smart phones and PDAs. Now users can access the same point in the Web from several different devices (office or home PC, cell phone, PDA, and so forth) throughout the course of a typical day. Consequently, for most users, what matters is the view a particular machine provides of the digital world. For instance, using SIM cards demonstrates that, for many users, the end-system is becoming less important than the access it provides to the digital world. In this sense, we are well on the way to computers "disappearing" and users being free to focus beyond them. Furthermore, for most users, computing and communication devices in these networks, such as cell phones, laptops or palmtops, are essentially free and are replaced relatively frequently. This is showing another important trend that Weiser associated with ubiquitous computing devices: many users view them as a commodity that they can find and use anywhere they travel. An important factor in forming this view is certainly the price and availability, as pointed out above.

Inspite of all the afore-mentioned rosy pictures, mobile computing is still a very young and evolving field of research. Though the platform of Web computing is quite well understood, the addition of mobility gave a new twist to the existing problems of distributed/Web computing because of mobility-related constraints, namely diminishing weight and size of devices, limited bandwidth, variation in network parameters, location awareness, limited battery power, less security, and so on. For example, SIM card represents only a partial solution to the implementation of Weiser's ubiquitous devices because users typically own only one SIM card and hence can't use multiple devices simultaneously. Moreover, users must consciously insert their SIM card into a handset- they can't just pick up and use any handset. Similarly, although laptops or phones are perceived as cheap, they are not usually left lying around for casual use in quite the way Weiser described. Also, wireless networking technology is not so mature as the Internet that people can assume its presence pervasively. The full body of knowledge on mobile computing is currently available in the conference/journal literature, and only some significant results have been codified in textbooks. They include research findings in broad areas, such as *mobile wireless networking* (location/mobility management, Mobile IP, ad hoc protocols, wireless TCP, mobile Internet), *mobile information access* (disconnected operation, bandwidth-adaptive file access, selective control of data consistency), *support for adaptative applications,* (trans-coding by proxies, adaptive resource management), *system-level energy saving techniques,* (energy aware adaptation, variable-speed processor scheduling, energy-sensitive memory management), and *location sensitivity* (location sensing, location-aware system behavior) [2].

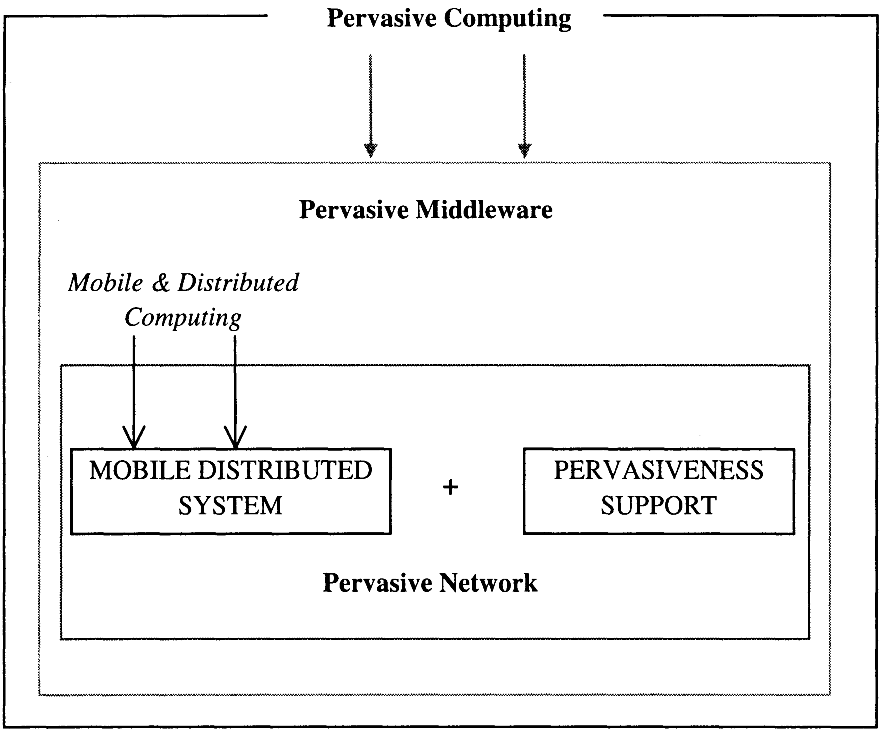


Figure 1.1 System view of PervComp

1.1.5 Pervasive Computing

Mobile computing is now making way for PervComp with the goal of omni-computing where it will be indistinguishable from our day-to-day life. PervComp defines a major paradigm shift from "anytime anywhere" computing (which is essentially a *reactive approach*) to "all-time everywhere" computing (which is a *proactive approach*) [3]-[9]. The first one, earstwhile known as MobiComp, implies that whenever you ask for your computing environment, you get it irrespective of your location and the time of request. The second one, now being known as PervComp, is a superset of the first one (Figure 1.1), implying that the computing environment is always with you, wherever you go, making you feel at home everywhere. The support for pervasiveness will come from interoperability (uneven conditioning [2]), scalability, smartness, and invisibility, on top of mobility. This will ensure that a user will not be reminded of the technology by its lack of presence during the hours of need, even if he/she is mobile. So the research issues in PervComp subsumes those of MobiComp model, and are much more complex and involved (see Figure 1 of reference [2] for more details) than both distributed computing and MobiComp.

1.2. PERVCOMP

PervComp can be defined as: *the overall infrastructural support needed to provide proactively a rich set of computing capabilities and services to a user (may be a nomad) every time everywhere in a transparent, integrated and convenient way.* It will be a convenient interface (not only access as in MobiComp), through a new class of appliances, to relevant information, with the ability to either take action on it or get acted upon by it, whenever and wherever necessary. Thus, PervComp will help manage information, the new currency of the global economy, quickly, efficiently, and effortlessly.

PervComp is about making our lives simpler. We increasingly rely on the electronic creation, storage, and exchange of personal, financial, and other confidential information, and demand the highest security for all these transactions. We are rapidly approaching an era where most consumer products contain an embedded computer and a tiny network interface (probably wireless). While the availability of ubiquitously "networked" goods is currently a novelty, it will soon be not only commonplace, but also all pervasive. For example, Ericsson and Electrolux are developing a refrigerator that will sense when it is low on milk and order for more milk directly from the supplier.

1.2.1 Introduction

Under the pervasive vision, the price of embedding a computer into a device becomes insignificant compared to the cost of manufacturing. Then users will access and retrieve information via a range of devices (e.g., phones, pagers, PDAs, office PCs, laptops, home entertainment systems, networked toasters, fridges, televisions, and indeed, any electronic device), with wide variations in memory capacity, power constraints, user interfaces and multimedia capabilities. Using these new classes of networked, intelligent and portable devices, PervComp aims to enable people to have a convenient complete access to relevant information stored on powerful networks, regardless of physical location, allowing them to accomplish an increasing number of personal and professional transactions everywhere, every time.

To provide a universal access to content, the information must be adapted to ensure compatibility to the device capabilities and minimize wastage of network bandwidth. Work in this area involves the development of intelligent and adaptable media presentation formats (such as XML, WML) that allow intelligent modification of content to suit different device characteristics and the development of appropriate "proxy" or gateway functionality (such as WAP gateways) which can transform/filter content based on a combination of network and device capabilities. Still there remain a number of questions unanswered. How do we manage quadrillions of PervComp devices? What communication strategies are needed? How do we effectively use networked food, clothing, paper, books, people, doors, cars and roads? And how do they interact with us?

1.2.2 Paradigm Shift

Simply speaking, PervComp is "omni-computing". It is "all-pervasive" by combining open standards-based applications with everyday activities. It removes the complexity of new technologies, enables us to be more efficient in our work and leaves us with more leisure time.

For over a decade, computer scientists have predicted the integration of computers and networks with the affordances of our daily life [1]. The development of hardware has today reached a point where this is technically viable, and it will shortly become financially accessible to average consumers. In the above vision, PervComp will be a part of everyday life, where computing will no longer remain a discrete activity bound to a desktop/laptop. It signifies a major paradigm shift from traditional computing, where users work through powerful host computers attached to fixed/mobile networks using PC-like end devices. In PervComp, users will work through a wide variety of devices, some with very limited capabilities and they may attach to an ad-hoc proliferation of wired/wireless networked appliances.

In a sense, traditional computing is more art than science because we are used to view computing devices as desktops, applications as programs that run on these devices, and the environment as a virtual space that a user enters to perform a task and leaves when the task is finished. On the contrary, PervComp presumes an altogether different vision where a device may be a portal into an application/data space, not a repository of custom software managed by the user. An application is a means by which a user performs a task, not a piece of software that is written to exploit a device's capabilities, and the computing environment is the user's information-enhanced physical surroundings, not a virtual space that exists to store and run software [6].

Environment (or, context), being an active part of the PervComp system, plays an important role here. The need for perceptual information about the present status of environment further differentiates PervComp from traditional computing. Sensing devices allow the system to have information about the state of the world, such as locations of people, places, things, and other devices in the environment. Having this information makes the interaction with the user seem more natural, when moving beyond the legacy of traditional isolated desktop model.

Although PervComp is similar to classical distributed computing in some instances, the differences are more pronounced than their similarities. The PervComp space is a combination of mobile and stationary devices that draw on powerful services embedded in the underlying network (PervNet) to achieve users' tasks. The result is a giant, *ad-hoc mobile distributed system*, with tens of thousands of devices and services coming in and going out. Due to this dynamic and distributed nature, existing approaches to conventional distributed computing are insufficient in at least *three* ways, when applied to PervComp. *First*, application data and functionality need to be kept separate, so that they can evolve gracefully in the global PervComp infrastructure. *Second*, applications need to be able to acquire any resource they need at any time, so that they can continuously provide their services in a highly dynamic environment. *Third*, PervComp requires a common system platform, allowing applications to be run across the range of devices and to be automatically distributed, installed and configured.

PervComp even defines a shift from MobiComp by combining mobile and non-mobile devices in a judicious manner to take advantage of both. In fact, it extends MobiComp to include each and every device (wired/wirelerss) for an omnipotent feeling as shown in Figure 1.1. Thus, beyond MobiComp, is the reach of PervComp, and this is certainly happening when the price one has to pay for "pervasiveness support" becomes insignificant compared to the cost of devices. In fact, PervComp is more personalized than simple MobiComp, and, at the same time, encompasses both wired and wireless technologies for wider coverage, better quality and pervasiveness. Far more than MobiComp, PervComp will wreak fundamental changes in the nature of computing, allowing almost every object encountered in daily life to be "aware", to interact, and to exist in both the physical and virtual worlds.

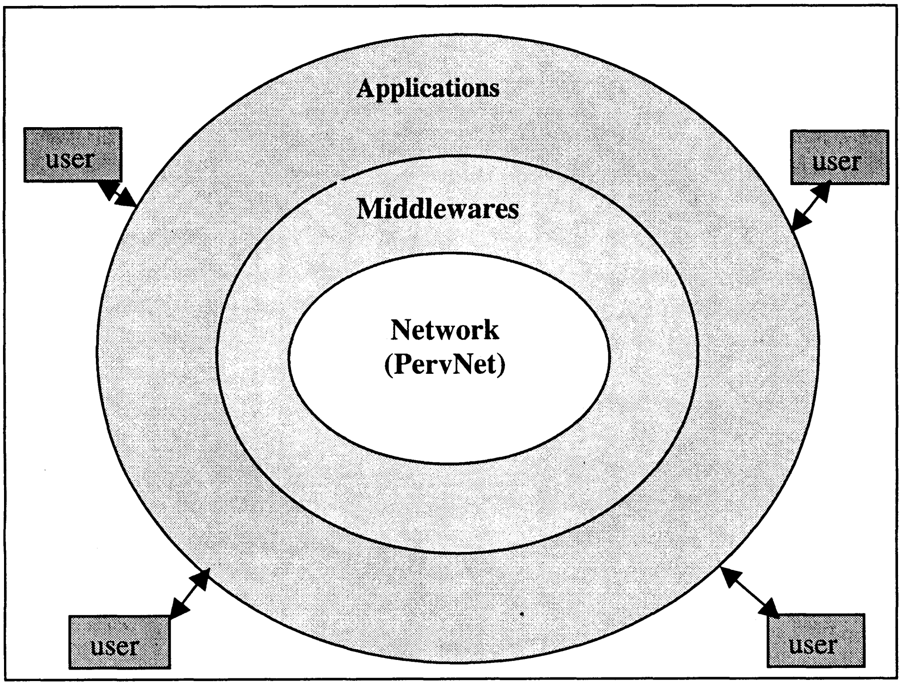


Figure1.2 Framework of PervComp

PervComp is not just about talking devices, such as laptops, workstations, mobile phones, palmtops, and PDAs; it is also about our daily life including appointments, meetings, leisure hours, family gatherings, weekend outings, four-wheelers, burglar alarms, refrigerators, or ovens. Pervasive means everywhere, and that include our bodies too. Bio-mechatronics, and medical telematics, are spreading at tremendous speed. So much so, that the space, where "human" ends, and "machine" begins, is becoming blurred in PervComp. In particular, PervComp dictates a new approach to interaction amongst hardware/software components, and between devices and human users.

1.3. PERVCOMP MODEL

Although the definition of PervComp is clear from a user perspective, what is required to build it is less clear. The technological advances, that are needed to build a PervComp environment, can be framed into *four* broad areas: *devices, networking, middleware, and applications* (Figure 1.2). To implement an architecture that can accommodate PervComp, all the four sets of technologies must be used judiciously. Although, in this book, we are primarily concerned about the core of this architecture, namely Pervasive Networking (PervNet), the two other areas are equally essential because, without them, there will not be enough users even to a successfully deployed network.

1.3.1 Pervasive Devices

An intelligent environment is likely to contain many different types of devices. First, there are traditional input devices, such as mice or keyboards, and traditional output devices, such as speakers or LEDs. Second, there are wireless mobile devices, such as handhelds, pagers, PDAs, cell-phones, palmtops etc. Third, there will be smart devices, such as intelligent refrigerators, sensitive floor tiles, bio-sensors, etc. Ideally, PervComp should encompass each and every device on the globe with active/passive intelligence in-built.

1.3.1.1 Smart Devices

These new intelligent appliances or "smart devices" are embedded with microprocessors that allow users to plug into intelligent networks and gain direct, simple, and secure access to both relevant information and services. These devices are particularly known as *pervasive devices.* As usual, pervasive devices will also fall under two general categories, namely *input* and *output.* Input devices include things such as sensors, active badge systems [7],[8], cameras, wall switches, sensitive floor tiles [9]. Output devices include home entertainment systems, wall-mounted displays, cell phones, sensors, robots etc. Most of the pervasive devices are as simple to use as calculators, telephones or kitchen toasters. Computation is completely embedded in these everyday objects, turning them into permanently connected residents in PervComp world. The MediaCup project [5] at the University of Karlsruhe is an experimental deployment of everyday objects activated in this sense. The guiding principle here is to augment objects with a digital presence, while preserving their original appearance, purpose and use. First objects prototyped are coffee cups equipped with a low-power microcontroller, embedded sensors, and wireless communication [5]. The embedded technology lets the cup sense their physical state and map sensor readings autonomously to a domain-specific model of the cup. This object model is broadcast at regular intervals over the wireless link to establish the object's digital presence.

1.3.1.2 Sensors

As the above terms suggest, an important subset of pervasive devices is a kind of sensors that are useful for automatic information gathering, transfer, and subsequent action taking. A very common example is GPS-based sensors, which provide location data that can be translated into an internal representation of latitude, longitude, and elevation. Due to the physics of receiving beacon signals, these sensors are, however, only useful in outdoor situations that are free of obstructions such as tall buildings. Similar to GPS, active badge systems [7] too are useful for providing positional information, but current systems lack a general mechanism for expressing arbitrary geometric information, particularly that which includes uncertainty. Another example is indoor beacon where sensors consisting of RF, IR or ultrasonic transceivers can determine the presence and perhaps location of small (usually powered) tags, which are attached to all objects of interest in the world, such as display, remote control, speakers, users, phones, printers, computers, etc. [8]. Vision being a natural sensing modality, stereo computer vision is another effective sensor for tracking the location and identity in the pervasive scenario. Moreover, vision does not require that the room's occupants carry or wear any special devices.

1.3.1.3 Handhelds

A very common handheld pervasive device is a *smart phone*, such as PCS Touchpoint of Sprint. Smart phones are nothing but a range of cellular telephones, which contain a microbrowser that can be used to access a subset of the Internet material. Another type of pervasive device is *PDA*, such as Palm Pilot of 3Com. PDAs are small and powerful devices with good portability, memory, and a display size of 160 by 160 pixels (6 cm x 6 cm). At a typical font size, this allows for approximately 13 lines of 40 characters each of content to be displayed. *Workpads* of IBM, such as Workpad c3, are also a kind of pervasive device. It is supplied to IBM by 3Com, and, hence, is similar to Palm range of PDAs.

These devices have a wide range of attachments available, including barcode scanners, modems, and GPS sensors. There are also ruggedized versions that are suitable for industrial applications. They come with built-in address books, calendars, calculators and e-mail, and have hundreds of third party applications available for productive use. Wireless PDAs, such as Palm VII of 3Com, add wireless connectivity to the Palm Pilot through an internal radio frequency (RF) transceiver, which enables it to function as a connected device. While the relatively low throughput of presently available radio networks (around 2 Kbs) limits the amount of information that can be transmitted (3Com suggests a norm of 40 bytes for the query, and 360 bytes for the response), there is a wide range of simple query-response applications for which the Palm VII is ideal. Palm VII will run the same applications as a Palm V or IBM WorkPad c3; however, this set of applications will not have direct access to the RF transceiver.

The number of pervasive devices is expected to multiply rapidly over the next few years. International Data Corp. (IDC) has predicted that, by 2003, the number of pervasive devices will exceed the estimated number of people (6 billion) worldwide. Specifically, there will be more than 300 million PDAs, 2 billion consumer electronic devices, such as wireless phones, pagers and set top boxes, and 5 billion additional everyday devices, such as vending machines, refrigerators, and washing machines embedded with chips connected to the PervNet. As a serious consequence of this proliferation, many of the current technologies have to be revamped in order to survive this techno-social revolution. Global networks like the Internet must be prepared not only to extend the backbone infrastructure to meet this anticipated demand, but to modify their existing applications so that devices become completely integrated into existing social systems.

1.3.2 Pervasive Network (PervNet)

PervComp, as visualized above, is aiming for a world in which every object, every building, and every body becomes part of network service. The explosion in pervasive connectivity is the prime reason behind companies' willingness to pay billions of dollars for attaining pervasiveness. But the question is how to achieve that. Is it just buying bandwidth? In the UK alone, a recent auction of just five bits of radio spectrum prompted bids totalling $25 billion. That's an awful lot of money to invest. But is that going to pay? It prompts one to ask: how should these companies plan such investments? We will elaborate on these issues in the next chapter and then make an attempt to highlight in the following chapters the existing technologies that fit into this architecture.

1.3.3 Pervasive Middleware (PervWare)

As we have seen in the cases of distributed computing and MobiComp, a shell of middleware is essential to interface between the PervNet kernel and the end-user applications running on pervasive devices. This PervWare will be responsible for keeping the users immersed in the PervComp space and for mediating all interactions with the PervNet kernel on behalf of the user (Figure 1.1). It will mostly be a bundle of firmwares and/or softwares executing in either client-server or peer-to-peer mode. For example, application development on Palm devices must be done in the 'C' language using tools such as Metrowerks' Code Warrior. 3Com's Palm VII applications use a query-response architecture. The user fills in a pre-defined query form and transmits the variable data through a proprietary wireless gateway (Palm.Net) to an application running on a Web server. The server returns a subset of HTML, which is displayed on the Palm VII.

When considering levels of sophistication for user interfaces, standard Web browsers represent the high end of the spectrum for pervasive devices. They make more use of colors, graphics and sophisticated controls than those typically expected on pervasive devices. MobiComp has already introduced microbrowsers, which are used in mobile phones. An example of a microbrowser is the popular UP.Browser from Phone.Com, which is implemented on a number of commercially available digital phones. The UP.Browser is capable of displaying HDML, a restricted subset of HTML. It is essential that when application developers create applications for use with pervasive devices, those same applications can still take full advantage of all of the features that a standard browser can support. Another good example is pervasive Java. Sun Microsystems demonstrated an early form of k-Java (a Java Development Kit for the Palm) at the Java One conference in 1999. Because these are intelligent devices, they are well suited to run intermittently connected applications, where the user works offline and occasionally connects to a server to synchronize data and execute any pending transactions.

Some of the intended functionalities of PervWare are: smartness, context-awareness, proactivity, transparency, mobility management, invisible interface, and adaptability. It is an important component of smart space that PervComp envisages for. The issues are related to operating systems and distributed systems, but with a bigger dimension because of the PervNet. We will touch upon these issues in Chapter 5.

1.3.4 Pervasive Applications

In every computing model, applications matter finally. PervComp is no exception to that. Deploying real life applications successfully is the ultimate goal of PervComp model too. But, here also, PervComp differs from its predecessors (namely, Web computing and mobile computing) considerably. Since it is more environment-centric, applications will guide the issues in PervWare and PervNet to a large extent. Applications will be pervasive, proactive, smart and adaptive. Fortunately, PervComp is fast maturing from its origins as an academic research area to a commercial reality, and applications are cropping up gradually.

IBM's T J Watson Research Laboratory has pioneered in demonstrating the broad range of possible (real life) pervasive applications using simple devices such as Palm Pilot and Workpad. These PDAs allow users to work offline (disconnected from the host system) for periods of time, and then synchronize with a server when it is available nearby. During synchronization, they transmit the work performed as a set of discrete transactions and receive any necessary updates. PDAs are excellent devices to run such an application as it is highly portable and may be used in areas which may have no cellular or telephone access.

Medical telematics is one of the fastest growing, and probably the most valuable, sector in telecommunications- the world's largest industry. Heart disease, on the other hand, is a mass problem. It's also a big business and has potential for pervasive applications. Suppose you give every heart patient an implanted monitor. It talks wirelessly to computers, which are trained to keep an eye open for abnormalities. Your body is very securely plugged into the PervNet. That's pervasive computing, surely. A similar kind of application that puts PervComp technologies directly into the service of improved quality of life is the assisted living complex constructed by EliteCare (www.elite-care.com) [4]. It gives residents as much autonomy and even responsibility for themselves and their environment as possible. It focuses on creating a personalized environment that avoids the traditional institutional care model used in nursing homes for the elderly who can no longer live unassisted.

Above examples are a few instances only, and a number of such instances exist in day-to-day's life. As pervasive devices will be richer in capability and potential, application will grow commensurately. Refrigerator ordering for milk or vegetables, dashboard guiding you through relatively free roads, health monitor telling you to go to a doctor, cellphone recording a call when you are visiting your ailing friend in a hospital, etc are some of the mundane examples cited in numerous papers [1]-[3]. The bottom line is that you cannot name an application where PervComp will not be present. Our point is that applications of PervComp will be indistinguishable from our daily life. Each and every application that we can think of should come under its purview because it is pervasive. Otherwise, it will not be able to disappear and will be utterly prominent being marked by its sheer absence.

1.4. ISSUES

As we have discussed already, PervComp, being a superset of MobiComp, not only subsumes the research issues of MobiComp but also opens up additional issues that are unique to itself. A majority of them is related to intelligence, pervasiveness, smartness, and invisibility. We discuss important ones here.

1.4.1 Perception (Context Awareness)

Today's devices are mostly context-insensitive. So they are distinguishable from human world. They cannot follow what is happening around them. Hence, they cannot take timely decisions, unlike human beings. On the contrary, perception (or, context awareness) is an intrinsic characteristic of the intelligent environment that is a prerequisite of PervComp. However, implementing perception introduces significant complications for PervComp, including the need to model uncertainty, perform real time data analysis, and merge data from multiple, possibly disagreeing, sensors. However, unless accurate, this context information may produce a complex or intrusive user experience. For example, unwanted intrusions could occur if your smart phone fails to perceive such things as an important meeting or a hospital indoor. To achieve perception, we need constant location monitoring, fast information processing, and accurate modeling of real world.

1.4.1.1 Location Informing

Gathering information about locations and their internal representations for management is an important issue. For instance, determining driving directions and delivering reminders [10] based on the user's location may be a task in PervComp. Some systems base their notion of location on semantic tags applied to network or electricity connections, e.g. "Ethernet tap 324 is in the living room." While it is possible to internally store the location of everything in latitude/longitude/elevation, the lack of an explicit uncertainty representation forces applications which query this model to assume some nominal uncertainty (e.g., typically the nominal GPS accuracy is of 15m).

This resolution may br insufficient for some tasks in the PervComp scenario. Additionally, if incompatible positioning technologies are available, it will be difficult to integrate them, as they may not express their measurements in the same coordinate frame or with the same uncertainty. As an alternative, instead of individual location information, we may also use collective information through vision.

1.4.1.2 People/Device Tracking

We are already conversant with issues related to location/mobility management in the context of MobiComp. But that was a reactive (discrete) approach. Tracking is similar to it in concept, but obviously more complex than location/mobility management simply because of its proactive (continuous) nature.

Knowing locations of people/devices continuously is important for the behavior of an intelligent environment. For example, if a wireless keyboard is near a certain person, it can be assumed that the person is producing keystrokes coming from that keyboard. The keystrokes can then be properly routed to that person's active application. Similarly, tracking a person is necessary to tell which keyboard (obviously the nearest one) he/she is using, if there are multiple keyboards in a laboratory. Therefore, tracking people and devices is the first step in exhibiting smartness.

Sensors (like GPS), attached to a device, are usually deployed to obtain information about the device or the person carrying the device. For example, RADAR [11] is an in-building location-aware system being investigated at Microsoft Research. RADAR allows radio-frequency (RF) wireless-LAN-enabled mobile devices to compute their location based on the signal strength of known infrastructure access points. Knowing the location of the devices allows components that are running on that device to provide location aware interfaces. It also provides a means for inferring the user's location.

Vision may also be used to find and/or track objects in a small space; for example, a camera mounted on the ceiling may be used to locate (follow) the wireless keyboard (person) in the laboratory room. The keyboard is detected in the image using a combination of color and shape cues. Vision can even resolve the location of a number of devices and users in a defined space well enough to infer, say a person's intent based on his or her position. It can maintain the identity of people in the room, allowing the room's devices to react to a specific person's personal preferences. It can even tell when a person stands or sits. Continuous location information can also be gained from systems that track beacons. Sometimes, tracking a person (i.e., his/her body-LAN) is easier than tracking individually each and every gadget he/she is carrying (i.e., connected to body-LAN).

1.4.1.3 Geometric Modeling

Previous systems for geometric modeling have typically tightly coupled the sensor modality with internal representation and the application (e.g. using GPS, or storing latitude/longitude). This is problematic both because it requires ongoing administration and also because it can break the shared metaphor between system and user. A more general system should decouple the sensor from the application, providing an internal representation, which can support a wide variety of both. Vision can be used to make a geometric model of the room. Images from the people-tracking cameras are used to make a floor plan of the room. For example, if a person plugs a light into an outlet in the den, but places the light in the living room, this new light would not appear on his/her room controls due to the limited geometric representation.

1.4.2 Smartness (Context Management)

Once the perception about the current context is achieved, next comes the question of the effective use of that in smart spaces [2]. In order to support richer interactions with the user, the system must have a deeper understanding of the physical space from both a sensory (input) and control (output) perspective. For example, it might be desirable for a smart system to provide light for a user as he/she moves around at night. To enable this, the system must use some form of perception to track the user, and then must be able to control all of the different light sources. Therefore, smartness involves accurate sensing (input) followed by intelligent controlling or action taking (output) between two worlds, namely machine and human. Perfect blending of these two worlds, which have been disjoint until now, was the theme of Weiser's vision [1]. This, in turn, will allow sensing and control of human world by machine world and vice versa. An example, taken from [2], is the automatic adjustment of heating, cooling and lighting levels in a room depending on occupant's electronic profile. Also, self-tuning of a TV picture based on viewer's mood and ambience is another example.

Smartness should encompass every individual object, irrespective of its position. To enable this, we need to embed communication and computing infrastructure everywhere, including building, streets, marketplace, offices, corridors, courtyard, highways and everything, either wirelessly or through wires. Then the whole world will be a big smart space wherein human beings are immersed. This infrastructure will be built upon the backbone of PervNet, which is the focus of this book.

1.4.3 Heterogeneity

As we have seen in the case of distributed computing, homogeneous implementation is not practicable for various technical and non-technical factors. Even standardization does not help as a single specification may lead to incompatible implementations. Conversion from one domain to another is a part of computing and communication. PervComp will also face the same music. Assuming that uniform and compatible penetration of environmental smartness is not achievable, masking heterogeneity (or, uneven conditioning [2]) in a user-transparent manner is extremely important for making PervComp invisible. For instance, there will always be a big difference between a sophisticated laboratory and a departmental store in terms of infrastructural smartness. This gap has to be filled up at some (say PervWare) level of PervComp so that the smartness jitter is smoothened out. Complete removal may be impossible, but restricting it below our tolerable limit is well within our reach by the complementary approach. In MobiComp, we have already achieved disconnected operation, thereby hiding the absence of wireless coverage from the user. The same concept may be borrowed to the PervWare to dynamically compensate for less smart (dumb) environments so that user does not feel any change at all. For PervNet, we have already faced protocol mismatch problem and learnt how to tackle the large dynamic range of architectural incompatibilities in order to ensure trans-network interoperability. But the real difficulty lies at the application front. Today, applications are typically developed for specific classes of devices or system platforms, leading to separate versions of the same application for handhelds, desktops, or cluster-based servers. Furthermore, applications typically need to be distributed and installed separately for each class of devices and processor family. As heterogeneity increases, developing applications that run across all platforms will become exceedingly difficult. As the number of devices grows, explicitly distributing and installing applications for each class of devices and processor family will become unmanageable, especially in the face of migration across the wide area.

1.4.4 Scalability

Future PervComp environments are likely to see the proliferation of users, applications, networked devices and their interactions on a scale that we have never experienced before. This will have a serious bandwidth, energy and distraction implications for users, and wireless mobile users in particular. As the degree of smartness grows, the number of devices connected to the environment as well as the intensity of man-machine interactions increases. From implementation perspective, scalability becomes an even more important issue for PervNet management and particularly for application design. The addition of new pervasive devices will increase network usage by many folds. The Internet explosion has already demonstrated that most existing information technology (IT) systems were not designed to handle rapid increases in demand. The traditional application development approach requires that applications need to be created for each new device. Even in the unlikely event that an enterprise could generate new applications as fast as new devices are added, there would be a tremendous value in solving the scalability problem, if they could write the application logic only once in a manner independent of devices (i.e., application portability).

A major issue, in regard to scalability, could be of *immediate visibility* for incoming devices. This necessitates that every new subscription registered by a client is guaranteed to receive a matching message sent as the next packet on a client's connection (a single server can provide immediate visibility). But it is not an easy task to maintain this semantics on a PervComp scale, where multiple servers will cooperate and when it would require synchronization of changes to subscription registries. The delayed propagation of both messages and subscriptions mean that this guarantee cannot be maintained for clients connected to different servers. However, a good point in handling scalability is *localization* [2], which goes against the theme of networking. If computing is present everywhere, it is always advisable to reduce distant interactions by replacing them with equivalent local interactions. Mirroring of websites is a major step towards this direction. But automatic handing off to nearby resource server, as an user moves around, is yet to be achieved because existing research efforts on scalability in distributed systems typically do not consider physical distance. But the situation is very different in PervComp where the environment will be overwhelmed by distant interactions unless the density of interactions diminishes with distance (much alike the inverse square law of nature [2]).

1.4.5 Invisibility

Ideally, PervComp will be invisible because of its complete disappearance from user's conscience. If you keep on getting the desired things before you think about it, you are bound to forget how this is happening. You have little time to ponder over it because you are used to it. For example, today wherever you go and whenever you want, you get electricity at your fingertip; so you take it as granted. Similarly, if you get computing everywhere every-time (i.e., you interact with it at the subconscious level), you are forced to be oblivious of its presence. It becomes invisible by its omni-presence. For example, if a user entering an office could have his/her "profile manager" node automatically discover the identity of the thermostat controller and "instruct" it to achieve the user's preferred temperature settings, then he/she forgets to thank the manager. At the implementation level, this requires self-tuning or auto-adjustment and anticipatory actions sometimes.

In practice, a reasonable approximation to invisibility is minimal human intervention i.e., user distraction at the conscious level. Human intervention is needed when the smart environment cannot self-tune itself according to user expectation in order to handle the situation automatically or the environment performs something that is unexpected of. This may require continuous learning on the part of the environment.

1.4.5.1 Self-tuning (Autoconfiguration)

To meet user expectations continuously, self-adjustment of the environment is compulsory. At the same time, objects must be capable of tuning themselves automatically in PervComp. Depending upon the extent of tuning needed, it can be implemented at different levels (such as application, PervWare, or PervNet) of PervComp. At the PervNet level, this may imply autoconfiguration of devices. Since the currently prevalent manual configuration approach will be too cumbersome and time-consuming for the dimension of PervComp environment, it will clearly need to use automated configuration techniques with the ability to dynamically reconfigure the PervNet as and when required. For instance, configuring a pervasive device with addresses, subnet masks, default gateways, DNS servers etc., when it joins the PervNet, without manual intervention will be crucial to the successful realization of the PervComp dream.

1.4.5.2 Anticipation (Proactivity)

In addition to providing a self-organizing capability, anticipatory moves are sometimes required on the part of the environment to interface invisibly with the human world. This may be a simple preventive measure or may be an indication of a future task. For example, on your way to airport if you are almost finished editing a large document, PervComp may trigger a dialog box in your laptop's screen (in anticipation that you want to e-mail the doc file) telling you to enter airport through Gate 15 where very few people are using the Internet (so available bandwidth is more) [2]. At the PervNet level, this implies that auto-configuration protocols must allow network nodes to distribute and query capability information dynamically. Similarly, when a person enters room A in an unknown laboratory and start typing a letter, it would be great if a message comes to his/her screen that printer is available only in room B. This is possible only if the visiting node could discover the printer through a process of cooperative advertisement and solicitation among all the nodes within the laboratory. Such cooperative capability dissemination is essential to the development of intelligent "environment-aware" applications.

1.4.6 Integration

Weiser's vision still seems like science fiction, primarily because the whole is more than the sum of its parts and the proper way of integration in existing systems is lacking. Though the components are already deployed in many environments, integrating them into a single platform is still unknown or poorly known. This integration problem is similar to the one already faced by the researchers in distributed computing; but, in PervComp, it is in a much bigger scale and dimension. As the number of devices and applications operating in PervComp environment increases, integration becomes more complex. For example, servers have to handle thousands of concurrent client connections, and would quickly approach the limits of their host capacities with the influx of pervasive devices. So we need a *confederation* of autonomous servers cooperating to provide services (i.e., routing messages at the PervNet level) to their consumers. This has severe reliability, quality of service (Qos), invisibility, and security implications for the PervNet.

Another example is the following. Satellite navigation (GPS) and information systems are standard in many high-end cars; several different means exist for detecting parking availability (for example, tapping parking lot's video surveillance camera and running an algorithm for detecting spaces); and it is possible to identify new shops using a neighborhood Web page or store guide. However, integrating them all into a single federation in Sal's world [1] uncovers a host of issues associated with deploying PervComp systems. The components from which to construct such systems might already be available, but they are typically conceived and operated independently, in the context of their own restricted view of the world. So, assuming that the "simple" problems associated with large-scale ad hoc software integration (such as naming, interface specification, fault tolerance, and configuration management) have all been solved in the literature of distributed computing, the focus is now primarily on the problems of creating integrated PervComp systems.

There is an obvious need for useful coordination between the components to ensure a reasonable user experience in a confederation. This coordination might range from traditional areas such as arbitrating screen usage to new challenges such as deciding which application may use the intensity of the light in a room to communicate with the user. Within an organization, business unit or site, federation usually requires universal availability, and is used as a means of providing reliability, scaling to large numbers of clients or to provide separate administrative authority over a sub-domain. Within a local area federation latency is significant. If a produced message is effectively multicast to a cluster of servers, each of which supports a group of subscribers, supporting large numbers of consumers is simply a matter of balancing the consumer connections evenly across a cluster of servers. But, beyond the bounds of an enterprise domain, for a wide area federation, access to messages is the primary requirement; a communication "backbone" allowing subscription to messages sent from anywhere in the world (or campus, or company) and publication of internal messages for global access. Finally, the routing of messages between servers introduces the possibility of messages from a single producer using multiple paths to reach a consumer, and hence arriving at a consumer out of order or duplicated.

There will be various distinct scenarios for federation in PervComp, distinguished mostly by usage requirements, with different trade-offs taken to address these issues in various contexts. However, while dwelling upon integration, one must also keep in mind the issue of interference. This interference is beyond the notion of physical interference and includes interference at the logical (software) level. For example, if two PervComp applications have conflicting requirements in terms of infrastructure services, they will need to resolve this conflict, ideally without user intervention. It seems reasonable to assume that future PervComp components will need to be both integration-friendly and interference-free for wide-scale deployment.

1.4.7 Socio-economic Concerns

Even if we assume that PervComp is technically realizable, numerous problems would still inhibit the deployment of such a personalized system. For example, location/context data can obviously contain sensitive information, such as the identity of people at the scene, either directly through recognition or indirectly through identification. So users' security and privacy are broken very often without a blink of eye. This is certainly unacceptable and might lead to litigations. Consequently, the location-tracking component could only deliver images, if it sought explicit consent from the people who might be identified, which clearly is technically and socially infeasible. Therefore, PervComp involves not only technical issues, but also a host of social, legal and economical issues. An obvious alternative to the above problem is to return only the specific information, removing the possibility of other components accessing sensitive information, thereby reducing the component's general usefulness in PervComp environment.

However, designing such components would still require care to avoid personal data spilling into public services. Also, when a PervComp application delivers some service, the cost of providing the service is distributed among numerous components. Such components might include the video system and its operators and the communications provider that enables the information to user. How do these service providers recover their costs? Hence, it is important to note that it is necessary to incorporate these factors into the infrastructure components that require careful design for perfect billing, charging, pricing, no legal implications, protecting user privacy and social acceptability. Finally, developing effective business models for PervComp systems will clearly be crucial to their success; yet, at best, system designers poorly understand this issue.

1.5. APPLICATION POTENTIAL

Examples of potential pervasive applications are galore in the literature starting from the story of Sal by Weiser in [1]. In fact, every paper on PervComp dwells with an example of potential pervasive applications. Jane and Fred provide two classic scenarios in [2]. We also present in this section an imaginary example illustrated in [12] to highlight the huge potential of PervComp applications. This story is inspired by Hiro's pizza box in [13].

Somewhere in Europe, there is a factory that produces canned food. Each can contains a tiny computer, a small amount of memory, and a short-range radio transceiver. It's a smart can, and, as part of their production, cans get embedded with a small amount of data such as the date of manufacture, the batch and can number, the alloy details etc. Once produced, these cans travel all over Europe. One batch of these cans is sent to Italy where they go to a tomato-canning factory and are filled with tomatoes. At this factory, as part of the canning process, the can gathers a little more data: it is full of diced Roma tomatoes, it was filled on a certain date as part of a particular batch, and it has a particular use-by date.

One of these cans of tomatoes gets exported to the USA. As it moves off the wharf, it is processed and its data content is translated from Italian to English. After a brief stint in a warehouse, it ends up on a supermarket shelf. At the supermarket, it inherits a little more information, such as the retail price and date of being placed on the shelf. At some point, your pantry knows to order the can, and one is sent to your house in the next delivery. Before the can leaves the store, the supermarket extracts the information it needs for stocktaking.

Some weeks later you are at your desk at work thinking about dinner, and decide that tonight you are going to cook a romantic meal for two. You look up your recipes, select one, and check your pantry for the necessary ingredients. Your tomatoes have cheerfully registered themselves to the pantry upon arrival, so it is able to report that all you need is some fresh basil that you can pick up on the way home. You are in no mood to work more, leave your desktop, grab your palmtop and walk out of office. The current state of your work gets silently transferred from your desktop to palmtop, in case you decide to resume work at home.

At the supermarket, you find the basil and drop it into the trolley, which updates the cumulative price of your selections. Noticing the screen's flicker, you glance down and see an advertisement for a free gift. As you collect it, your wristwatch flashes to inform you that your friend has already come to your house. Finally done, you push the trolley through the checkout, where your account is debited for the total, and your home address is attached to your items. You push the trolley onto the track for delivery and rush home as the store delivers the shopping for you.

At home you begin to cook, placing the opened can of tomatoes from the pantry onto the table. The can reports that it has been opened (after detecting the pressure differential). You have been meaning to get the auto-light on your gas stove fixed for weeks now and seemingly every time you want to light it you cannot find the matches. You ask the kitchen to locate the nearest box for you: there is one in the cutlery drawer. You have had enough though, so you direct the kitchen to include the stove repair into your budget. Your stove knows not to hassle you again.

Having enjoyed your meal with your friend, you turn on the television but during the first ad break a scrolling message from the kitchen appears at the bottom the screen telling you that there is an open can of tomatoes that is been getting warm for over two hours. You swear briefly, but are at least glad the house did not interrupt while you were busy. It knows you are not watching an important show and it did have the decency to wait for an ad break. You go to the kitchen and put the can into the fridge, pausing briefly to put the matches back on the fridge where you expect them.

Three days later you wake up and struggle to the kitchen for a cup of coffee. As you grab the milk, you see the fridge's display panel has a number of messages for you. You will deal with the emails later but notice that the fridge is complaining that there is a can of tomatoes that is getting beyond its prime. At first you cannot find them, but the fridge locates them behind the last of the beer, and you grab the can and blend them. Enjoying your tomato juice with your coffee, you begin a casual cleanup and throw the empty can into the recycling unit. The recycling unit strips any personal information from the can, and, noticing the alloy content, ensures that it gets picked up for recycling. Some time later the can is shipped back to its factory for recycling.

This is a glance of PervComp and you name the application included in the above story, which does not come under it.

1.6. PERVASIVE INITIATIVES

It all probably began, way back in early nineties, with the ParcTab effort at Xerox PARC by the team of Mark Wieser. Though it was not accepted well by the research community at that time, it actually marked the beginning of PervComp. Thereafter, various attempts were made at different times under varying names, such as wearable computing, ubiquitous computing, invisible computing etc. Recently, some serious efforts have emerged at both academics and industry under the direct designation of "PervComp". They appear to pick up where the ParcTab effort left off. We briefly discuss some of them (not exhaustive) in this section now.

1.6.1 ParcTab

Perhaps the first seminal project in the arena of PervComp was the ParcTab [14] project of Xerox at their Paulo Alto Research Center (PARC). In the ParcTab project, much attention was given to an application travelling with the user, and being accessible from mobile devices. This is an example of devices acting as portals into an information space and lends credence to the proposed vision of PervComp. Unfortunately the ParcTab project ended before it could realize its potential mainly because of the non-availability of matching hardware technology during that period. Moreover, at that time, applications were often custom coded, and the project focused on the utility of pervasive applications rather than application development and an accompanying application model. Consequently, the project fell short of any implementation whatsoever.

1.6.2 Aura

Project Aura [15]-[17] at Carnegie Mellon University (http://www-2.cs.cmu.edu/~aura/) is about Distraction-free Ubiquitous Computing. It will design, implement, deploy, and evaluate a large-scale system demonstrating the concept of a "personal information aura" that spans wearable, handheld, desktop and infrastructure computers. Basically, it aims to develop a PervComp system, named Aura, whose goal is to provide each user with an invisible halo of computing and information services that persists regardless of location. Meeting this goal will require efforts at every level: from the hardware and network layers, through the operating system and middleware, to the user interface and applications. Project Aura will fundamentally rethink system design to address them.

Aura is a large umbrella project with many individual research thrusts contributing to it, including Task-driven Computing, Energy-aware Adaptation, Intelligent Networking, Resource Opportunism, Speech Recognition, Language Translation, Augmented Reality, Multi-modal User Interfaces, Nomadic Data Access, Wearable computers, User Interface Adaptability, Data and Network Adaptability, Software Composition, Proxies/Agents, Collaboration, Wireless networking, Security and privacy, User/Virtual Space Interaction, Evaluation Metrics and Methodologies. In fact, it is evolving from CMU's earlier mobile distributed system projects, namely Darwin (application aware networking), Spot (wearable computers), Coda (nomadic highly available file access) and Odyssey (OS support for agile application aware adaptation) [16]. At the core of Aura, there is an intelligent network Darwin (i.e., PervNet), on top of which runs Coda and Odyssey. Coda supports nomadic file access, and Odyssey performs resource adaptation. Both Coda and Odyssey (i.e., PervWare) are being enhanced substantially to meet the demands of PervComp. For Odyssey, these changes are sufficiently extensive to result into a new system called Chroma. Two more components, Prism and Spectra [2], which runs above Coda/Odyssey layer, are being created specifically for use in Aura. Spectra provides support for remote execution. Prism is the final interface between applications and users. It handles task support, user intent and high-level proactivity. Additional components are likely to be added over time since Aura is relatively early in its design. In short, the emphasis of Aura is on PervWare and application design.

1.6.3 Endeavour

The Endeavour Project in the University of California at Berkeley (http://endeavour.cs.berkeley.edu/) is another academic effort for understanding PervComp. The project, named after the ship that Captain Cook sailed on his explorations of the Pacific, is envisioned as an expedition towards "Charting the Fluid *Information Utility*" [18]. The focus of this expedition is the specification, design, and prototype implementation of a planet-scale, self-organizing, and adaptive *Information Utility* (i.e., PervComp environment). Fluid information utility is everywhere and always there, with components that "flow" through the infrastructure, "shape" themselves to adapt to their usage, and cooperate on the task at hand. Its key innovative technological capability is its pervasive support for fluid software. That is, the ability of processing, storage, and data management functionality to arbitrarily and automatically distribute itself among pervasive devices and along paths through scalable computing platforms, integrated with the network infrastructure. It can compose itself from pre-existing hardware and software components, and can satisfy its needs for services while advertising the services it can provide to others. It can also negotiate interfaces with service providers while adapting its own interfaces to meet "contractual" interfaces with components it services. The fluid paradigm will enable not only mobile code, but also nomadic data, which are able to duplicate itself and flow through the system where it is needed for reasons of performance or availability.

The *Information Utility* will be designed to support, and to integrate with infrastructure services of processing, storage, and information management, a great diversity of pervasive devices. These will include radical devices like MEMS-sensors/actuators and other capture and display devices that go well beyond the straight-forward extrapolations of today's server, desktop and portable computers. This PervComp architecture will be stressed by using it to enable demanding applications that support collaboration and learning in virtual and physically enhanced activity spaces. It will be designed and evaluated using innovative tools and comprehensive methodologies that are based on formal methods that span hardware and software, optimize the design for decomposition into reusable components with contractual yet adaptive interfaces, and verify the correctness and safety of the whole artifact being designed.

The mission of the project is to achieve nothing less than radically enhancing human understanding through the use of information technology, by making it dramatically more convenient for people to interact with information, devices, and other people. It will achieve this by developing the revolutionary *Information Utility*, able to operate at planetary scale. To validate the architecture, Endeavour will stress it under demanding applications for rapid decision making and learning. In addition, it will develop new methodologies for the construction and administration of systems of this unprecedented scale and complexity to effectively amplify and leverage human intellect.

1.6.4 Oxygen

Project Oxygen is the initiative of MIT (http://www.oxygen.lcs.mit.edu/) towards PervComp. The vision is that, in the future, computation will be freely available everywhere, like oxygen in the air we breathe. The project rests on an infrastructure of mobile and stationary devices connected by a self-configuring network (i.e, PervNet). This infrastructure supplies an abundance of computation and communication, which is harnessed through several levels (system, perceptual, and user) of software technology to meet user needs. It is focusing on eight environment-enablement technologies. The first is a new mobile device, the H21, which relies on software to automatically detect and re-configure itself as a cell phone, pager, network adapter or other type of supported communication device. The H21 is a good example of a mobile device that acts as a portal. The second and third technologies are the E21, an embedded computing device used to distribute computing nodes throughout the environment, and N21, network technology needed to allow H21s and E21s to interact. These provide some of the load- and run-time requirements described in [19]. The final five technologies underlying Oxygen are all aimed at improving the user experience: speech, intelligent knowledge access, collaboration, automation of everyday tasks, and adaptation of machines to the user's needs. Inherent in these technologies is the belief that shrink-wrapped software will disappear as an application delivery mechanism. More dynamic mechanisms will be used instead. The emphasis is on understanding what turns an otherwise dormant environment into an empowered one. Users of an empowered environment shift much of the burden of their tasks to the environment.

The project objectives [20] tell that Oxygen system must be *pervasive* (everywhere, with every portal reaching into the same information base), *embedded* (it must live in our world, sensing and affecting it), *nomadic* (its users and computations must be free to move around according to their needs), and *eternal* (it must never shut down or reboot). Components may come and go in response to demand, errors, and upgrades, but Oxygen as a whole must be non-stop and forever. The abundance of computation and communication to users is brought through natural spoken and visual interfaces, making it easy for them to collaborate, access knowledge, and automate repetitive tasks. Oxygen will help people *do more by doing less* by blending it into their lives, customizing itself to meet their needs, being accessible through natural perceptual interfaces, and making it easy for people to do the tasks they want.

1.6.5 Portolano

The Portolano Project is an initiative of the University of Washington (http://portolano.cs.washington.edu/). It seeks to create a testbed for investigation into the emerging field of PervComp. It emphasizes invisible, intent-based computing. The intentions of the user are to be inferred via their actions in the environment and via their interactions with everyday objects. The devices are so highly optimized to particular tasks that they blend into the world and require little technical knowledge on the part of their users.

The project focuses on three main areas: Infrastructure, Distributed Services and User Interfaces [21]. *User Interfaces*: New modes of interaction such as user movement, proximity of devices, and embodied information presentation will augment the keyboard, pen, audio, and video interfaces we see today. The challenge is maintaining task-oriented consistency across physical devices while managing the multiple interfaces in a coherent manner. Also, the focus must shift to user intent and expectation and away from the execution of explicit commands. Data gathered from a variety of location sensors, identification tags, and on-line services, will augment or replace many user directives common today. *Infrastructure*: The networking fabric must provide robust data transfer with replication and discovery as well as the ability to marshal computing resources at internal network nodes. Users must be able to count on their data arriving where it needs to go without their direct intervention. The network must be data-centric in that transmission, routing, authentication, and resource reservation should be handled independently of the location of the user who injected the data. Intermittent wireless connectivity and transmission cost optimizations are examples of decisions for which the user should simply provide guidance once rather than for each use. *Distributed Services*: Rather than abstract capabilities, emphasis must be placed on applications to which users can easily relate. Different user interfaces and agent technologies, appropriate to their contexts, should be able to reach the same services. For example, a scheduling service may span several pieces of network infrastructure yet should be available via home display, PDA, auto PC, and a phone with voice recognition and synthesis. To facilitate service deployment and consumer choice, these services must be more openly organized into horizontal layers rather than the vertically integrated monolithic services of today.

In short, Portolano proposes an infrastructure based on mobile agents that interact with an application and the user, and applications must be developed to utilize the agents. Devices are portals into the environment. However, their tasks are implicitly defined, and the portals capture user input, and reflect that input to the application. In networking, Portolano considers data-centric routing, which facilitates automatic data migration among applications on behalf of a user. Data becomes "smart", and serves as an interaction mechanism within the environment.

1.6.6 Sentient Computing

Sentient computing (i.e., PervComp) at AT&T Laboratories, Cambridge, UK (http://www.cam-orl.co.uk/spirit/) is a new way of thinking about user interfaces using sensors and resource status data to maintain a model of the world which is shared between users and applications. Because the world model of sentient computing system covers the whole building, the interfaces to programs extend seamlessly throughout the building, as well as obvious applications like maps, which update in real time, and computer desktops, which follow their owner around. This leads to some surprising new kinds of application, like context-aware filing systems, and smart posters. This is called shared perception. By acting within this world, we would be interacting with programs via the model. It would seem to us as though the whole world were a user interface. While people can observe and act on the environment directly, application programs observe and act on the environment via the world model, which is kept up to date using sensors and provides an interface to various actuators. If the terms used by the model are natural enough, then people can interpret their perceptions of the world in terms of the model, and it appears to them as though they and the computer programs are sharing a perception of the real world.

The technological challenges for sentinent system are: creating an accurate and robust sensor system which can detect the locations of objects in the real world; integrating, storing and distributing the model's sensor and telemetry information to applications so that they get an accurate and consistent view of the model; and finding suitable abstractions for representing location and resource information so that the model is usable by application programs and also comprehensible by people.

To solve these problems, they have built an *ultrasonic location system*, which provides a location accuracy of about 3 cm throughout a ten thousand square foot building, making it the most accurate large-scale wireless sensor system in the world. They have built a distributed object model, which integrates location and resource status data for all the objects and people in our building. They have also built a spatial monitoring system to implement an abstraction for expressing spatial relationships, which lets applications detect spatial relationships between objects in a way that seems natural to human users.

The location and resource status data for managing the world are represented by a set of persistent CORBA objects implemented using *omniORB*, their own GPL-ed CORBA ORB. Each real-world object is represented by a corresponding CORBA software object. Around 40 different types of object are modelled, each by its own CORBA object type; for example, the system includes the types: Person, Computer, Mouse, Camera, Scanner, Printer, Phone and so on. Along with the location of the real object, each software object makes available current properties of the real object, and provides an interface to control the real object. For example, a scanner can be set up and made to perform a scan by an application via its corresponding Scanner software object. The set of all these persistent CORBA objects make up the world model that is seen by applications. The objects themselves take care of transactions, fail-over, session management, event distribution and all the other issues, implicit in a large-scale distributed system, presenting a simple programming interface to the applications. Location data is transformed into containment relations by the *spatial monitor* for programming with space. Objects can have one or more named spaces defined around them. A quad-tree based indexing method is used to quickly determine when spaces overlap, or when one space contains another, and applications are notified using a scalable event mechanism.

1.6.7 CoolTown

The PervComp project initiative at HP Laboratory is know as CoolTown (http://www.cooltown.com). It is well known that the convergence of Web technology, wireless networks and portable client devices provides new design opportunities for computer/communications systems. Although the web infrastructure was never conceived as a general distributed systems platform, its ubiquity and versatility have opened up attractive opportunities for large-scale application deployment. CoolTown is exploring these opportunities through an infrastructure to support "web presence" for people, places and things. It puts web servers into things like printers and put information into web servers about things like artwork. It groups physically related things into places embodied in web servers. Using URLs for addressing, physical URL beaconing and sensing of URLs for discovery, and localized web servers for directories, it can create a location-aware PervComp system to support nomadic users. On top of this infrastructure, it can leverage the Internet connectivity to support communications services. Most of the work in CoolTown has focused on extending Web technology, wireless networks, and portable devices to create a virtual bridge between mobile users and physical entities and electronic services.

CoolTown bridges the Web and the physical world we inhabit, providing a model for supporting nomadic users without a central control point. CoolTown visions that the physical world and the virtual world would both be richer if they were more closely linked. Currently the Web is largely a *virtual* space: a space of web "sites", online "malls", and chat "rooms". These virtual locations have little correspondence with physical spaces. While much of the information on the Web describes the world we physically inhabit, there are few systematic linkages to real world entities. This is unfortunate, because most of our activities concern physical objects other than computers. This project describes how we could have systematically integrated web services to enhance communications with mobile people, to provide location-specific services in the places that they visit, and to provide interaction with the things that they encounter. To help users and developers formulate a common model of how these systems behave, CoolTown describes them as supporting "web presence". Web presence is the representation of people, places and things on the web. It extends the "home page" concept to include all physical entities and to include deliberate and automatic system supported correlation of the home page or *point of web presence* with the physical entity

1.6.8 eBiquity

The eBiquity Group, a research organization at University of Maryland at Baltimore County (http://research.ebiquity.org/), explores the interactions between mobile, pervasive computing, multi-agent systems and artificial intelligence, and e-services. Group members have research interests in the underlying areas, such as distributed systems, mobile networking and systems, data management for pervasive/mobile systems, ad-hoc networks, knowledge representation and reasoning, personalization, web/data-mining, multi-agent systems and security. Much of their research is driven by applications in the e-services area: e-commerce, m-commerce, home-automation, wireless web etc.

1.6.9 One.world

Another research effort from the University of Washington is *one.world* (http://one.cs.washington.edu/), a system architecture for PervComp. It is implemented mostly in Java and makes liberal use of object-oriented functionality. It keeps data and functionality separate by introducing a new, higher-level abstraction to group the two. Data is represented by tuples, which essentially are records with named and optionally typed fields, while functionality is provided by components, which implement units of functionality.

Environments serve as the new unifying abstraction. They are containers for stored tuples, components, and other environments, providing a combination of the roles served by file system directories and nested processes in more traditional operating systems. Environments make it possible to group data and functionality when necessary. At the same time, they allow for data and functionality to evolve separately and for applications to store and exchange just data, thus avoiding the two problems associated with objects discussed above. In *one.world*, applications need to explicitly bind all resources they use, including storage and communication channels. Leases are used to control such bindings and, by forcing applications to periodically renew them, provide timeouts for inaccessible or unavailable resources. While leases have been used in other distributed systems, such as Jini, to control access to remote resources, we take them one step further by requiring that all resources be explicitly bound and leased. Furthermore, resource discovery in *one.world* can use late binding, which effectively binds resources on every use and thus reduces applications' exposure to failures or changes in the environment. Further information on *one.world*, including a source distribution, is available at http://one.cs.washington.edu/.

1.6.10 EasyLiving

EasyLiving [22] is a PervComp project of the Vision Group at Microsoft Research (http://research.microsoft.com/easyliving/) for the development of architecture and technologies for intelligent environments. This environment will allow the dynamic aggregation of diverse I/O devices into a single coherent user experience. Components of such a system include middleware (to facilitate distributed computing), world modelling (to provide location-based context), perception (to collect information about world state), and service description (to support decomposition of device control, internal logic, and user interface).

The key features include: XML-based distributed agent system using *InConcert* [22], Computer vision for person-tracking and visual user interaction, Multiple sensor modalities combined, Use of a geometric model of the world to provide context, Automatic or semi-automatic sensor calibration and model building, Fine-grained events and adaptation of the user interface, Device-independent communication and data protocols, and Ability to extend the system in many ways. InConcert is a middleware solution that addresses these issues. InConcert provides asynchronous message passing, machine independent addressing and XML-based message protocols. Much of the information provided to the Geometric Model (and other attributed based directories) is data gained from the world through sensors. While much of this information could be entered into databases by hand, the more interesting case is when data is dynamically added and changed while the system is running. This data is gained from physical sensing devices that are attached to computers running perception components.

The EasyLiving system can currently handle a single room and tens of devices with dynamic changes to their configuration. The system has evolved to the point that user interface issues can now be more rigorously examined. As EasyLiving evolves, it is expected that input and output devices will no longer be tied to a single machine or application but rather be able to flexibly support user interaction across a wide variety of tasks and modalities. Future work will build on this architecture, further exploring the migration of computing from the desktop and into everyday living.

1.6.11 pvc@IBM

IBM is at the vanguard of PervComp (they call it *pvc*, http://www-3.ibm.com/pvc/), spearheading consortiums and initiatives for open standards that will enable continued growth and development of PervComp technology. IBM is working with PervComp hardware vendors such as Palm Inc. (www.palm.com), Symbol Technologies (www.symbol.com), and Handspring (www.handspring.com). Using their expertise with complex information technology, IBM shows how to leverage its knowledge of business processes and ability to analyze enterprise data into an unrivalled perspective on business problems and solutions across the global economy, when businesses around the globe are using PervComp to satisfy customers, to increase the convenience of doing business, to create customer loyalty, and to build partnerships. Their *Quick Start Engagements* [23] software is customized to the needs of specific industries, allowing your business to realize fast results with a modest initial investment. And, once you have analyzed the results, you can expand your pervasive strategy locally or globally. Thus, you can bring pervasive solutions to your customers who are looking for wireless and mobile extensions to their e-business applications. *WebSphere Everyplace Access* software extends e-business applications to a growing range of wireless and connected emerging pervasive devices across a variety of networks and connectivity. IBM is organizing a conference on PervComp [http://www.pervasive2002.org] where some good papers will be presented. IBM also maintains an excellent glossary of PervComp terms at http://www-3.ibm.com/pvc/tech/glossary.shtml.

1.7. SUMMARY

As described in the above sections, PervComp refers to the presence of an all-pervasive digital environment that is sensitive, adaptive, and responsive to the human needs. It can be characterized by the following basic elements: pervasiveness (ubiquity), transparency (invisibility), and intelligence (smartness). Self-tuning and proactivity are the key features of the smart space, which is achieved by combining knowledge from different layers of the system. Seamless integration of component technologies into a system makes the whole much greater than the sum of the parts.

The difficult problems lie in architecture, component synthesis and system-level engineering. Hardware must become adaptable, scalable, and portable. It should also be stream-efficient to provide computational resources that are both energy-efficient and powerful for a variety of computational tasks. Software and network protocols must become adaptable to flexibility, spontaneity, and heterogeneity. For example, interoperability demands smooth vertical hand-offs among communication technologies. Heterogeneous traffic has to be efficiently routed in response to application demands, through nodes that differ in connectivity, computational power, and resources. Services and software objects must be named by intent instead of addresses; for example, "the nearest Internet server", rather than by its IP address, which requires service location protocols. Above all, PervComp must be secure enough for people to use it without any hesitation.

It should be clear by now that, for PervComp to succeed, it must address many challenges, and as a consequence, the relevant research covers several areas including hardware, software, and networking. Fortunately, all basic component technologies exist today. In hardware, we have devices (handhelds, laptops, cellphones and so on), sensors, smart appliances, etc; in software, we have signal processing, object-orientation, compilers, etc; in networking, we have the Internet, LANs, UMTS, mobility management, ad hoc routing, etc. In the near future, thanks to this promising research, our homes will have a PervNet of intelligent devices providing us with information, communication, and entertainment transparently. We shall learn more about them in following chapters.

REFERENCES

[1] Weiser M., "The Computer for the 21st Century", Scientific American, September, 1991, (reprinted in IEEE Pervasive Computing, Vol. 1, No. 1, pp. 19-25, Jan-Mar 2002).

[2] Satyanarayanan M., "Pervasive Computing: Vision and Challenges", IEEE Personal Communication, Vol. 8, No. 4, pp.10-17, Aug 2001.

[3] Special inaugural issue on *Reaching for Weiser's Vision*, IEEE Pervasive Computing, Vol. 1, No. 1, Jan-Mar 2002.

[4] Stanford V.,"Using Pervasive Computing to Deliver Elder Care", IEEE Pervasive Computing, Vol. 1, No. 1, pp. 10-13, Jan-Mar 2002.

[5] Beigl M., Gellersen H. W., and Schmidt A.,"Mediacups: Experience with Design and use of Computer Augmented Everyday Objects", Computer Networks, Vol. 35, No. 4, pp. 401-409, Mar 2001.

[6] Banavar G., et. al. "Challenges: An Application Model for Pervasive Computing", Proc. of the Sixth Annual ACM/IEEE International Conference on Mobile Computing and Networking (Mobicom 2000).

[7] Want R. and Hopper A., "Active Badges and Personal Interactive Computing Objects", IEEE Transactions on Consumer Electronics. Vol 38. No.1, Feb. 1992, pp.10-20.

[8] Ward A., et al, "A New Location Technique for the Active Office", IEEE Personal Communications, Vol. 4, No. 5, Oct. 1997, pp. 42-47.

[9] Addlesee, M.D. et al, "ORL Active Floor", IEEE Personal Communications, Vol.4, No.5, October 1997, pp. 35-41.

[10] Marmasse N., and Schmandt C., "comMotion: a context-aware communication system", http://www.media.mit.edu/~nmarmas/comMotion.html .

[11] Bahl P. and Padmanabhan V. N., "RADAR: An In-Building RF based User Location and Tracking System", Proceedings of IEEE INFOCOM 2000, Tel-Aviv, Israel, March 2000.

[12] Arnold D., et. al., "Discourse with Disposable Computers: How and why you will talk to your tomatoes", Proceedings of the Embedded Systems Workshop Cambridge, Massachusetts, USA, March 29–31, 1999.

[13] Stephenson N., Snow Crash, Bantam Press, 1992.

[14] Schilit B., Adams N., Gold R., Tso M., and Want R., "The PARCTAB Mobile Computing System", Proceedings of the Fourth Workshop on Workstation Operating Systems, pages 34-39, October 1993.

[15] Sousa, J.P., and Garlan, D., "Aura: an Architectural Framework for User Mobility in Ubiquitous Computing Environments" Proceedings of the 3rd Working IEEE/IFIP Conference on Software Architecture 2002, Montreal, August 25-31, 2002.

[16] Flinn, J., and Satyanarayanan, "M. Energy-aware Adaptation for Mobile Applications", Proceedings of the 17th ACM Symposium on Operating Systems and Principles. Kiawah Island, SC, December, 1999.

[17] http://www-2.cs.cmu.edu/~aura/

[18] http://www.cs.berkeley.edu/~randy/Endeavour/

[19] Dertouzos M., "The Oxygen Project", Scientific American, 281(2):52-63, August 1999.

[20] Brown E. S., "Project Oxygen's New Wind", Technology Review, December 2001. (http://www.technologyreview.com/articles/4152.asp)

[21] Esler M., Hightower J., Anderson T., and Borriello G., "Next Century Challenges: Data-Centric Networking for Invisible Computing- The Portolano Project at the University of Washington", Proceedings of the Fifth ACM/IEEE International Conference on Mobile Networking and Computing, pages 256-262, August 1999.

[22] Shafer S., et al, "The New EasyLiving Project at Microsoft Research", Proceedings of the 1998 DARPA / NIST Smart Spaces Workshop, July 1998, pp.127-130.

[23] http://www.developer.ibm.com/pvc/index.html.

Chapter 2

Pervasive Networking

It has already been mentioned in the previous chapter that PervComp, simply speaking, is PervNet plus computing support (i.e., middlewares and applications). To start us on the road towards understanding what is PervNet, this chapter does three things. First, it introduces the idea of PervNet architecture, which lays the foundation for the rest of the book. Second, it explores the properties (or, attributes) that PervComp applications demand from PervNet. Finally, it introduces some of the key elements in the implementation of PervNet.

2.1 INTRODUCTION

PervComp promises a computing infrastructure that seamlessly and ubiquitously aids users in accomplishing their tasks and that renders the actual computing devices and technology largely invisible. The basic idea behind PervComp is to deploy a wide variety of smart devices throughout our working and living spaces. These devices coordinate with each other to provide users with universal and immediate access to information and support users in completing their tasks using a pervasive network, called PervNet in this book. Fortunately, this *networking infrastructure*, which is necessary to realize the vision of PervComp, is increasingly becoming a reality.

It all started with computer communication (ARPANET) [1] way back in 1979. Then we saw the merging of computer networks with communication networks and the emergence of the INTERNET [1], [2] as a seamless internetworking platform. Wireless mobile networks [3] revolutionized the scenario in late nineties with its concept of tetherless communication. Now, at the dawn of the new millennium, the idea of integrating all these networks (Figure 2.1), which have matured individually, is promising an all-pervasive platform of networks to users who are already accustomed to full-fledged global services in the wired world (e.g., PSTN) and limited anytime anywhere services in the wireless world (e.g., global roaming in cellular phones).

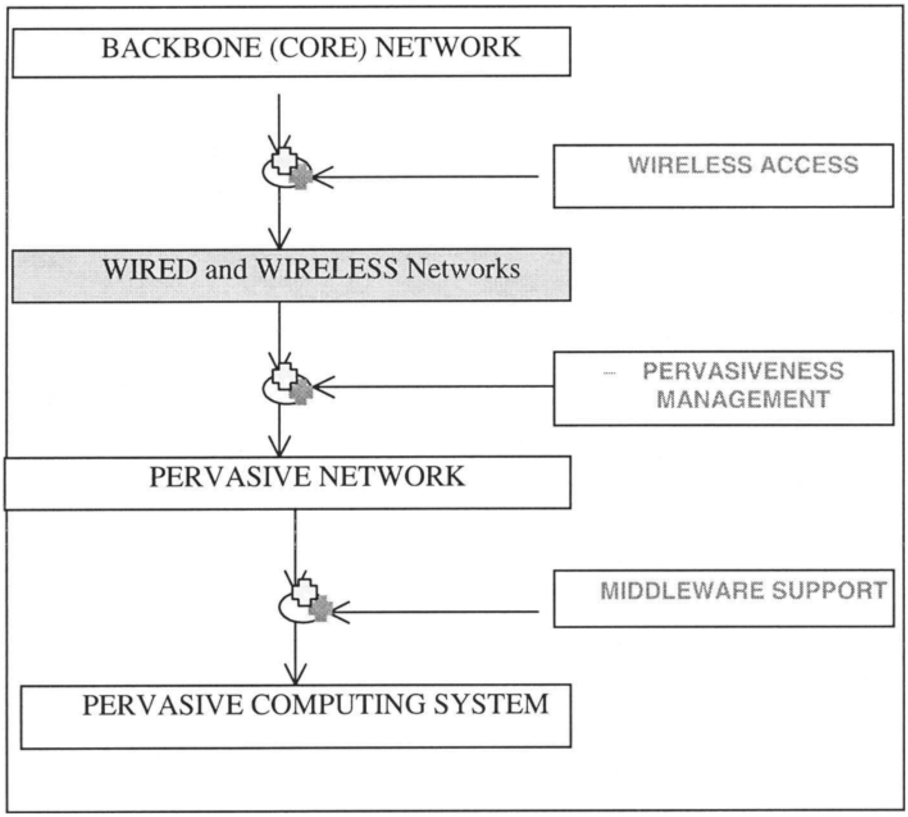


Figure 2.1 Network view of PervComp system

Traditionally, a network topology is carefully crafted and each router, switch or bridge is manually configured according to its fixed place in the network [1]-[3]. Traditional networks are typically static or (at the most) exhibit only host mobility, which is limited to the last hop so far. But PervNet will not follow this legacy and may contain ad-hoc proliferation of networks without manual intervention, many of whose nodes will be acting as mobile routers. It will be ad-hoc and dynamic in its true sense. Centralized management schemes will not work anymore, as architecture and protocols will not be fixed. So the immediate question that comes into mind is how to model this kind of network. An attempt is made in the following sections to define it as much understood at present.

2.2 NETWORKING INFRASTRUCTURE

2.2.1 Structure of PervNet

The envisaged structure of PervNet will be very simple, consisting of a core of backbone (wired/wireless) network and a shell of access (invariably wireless in case of mobility) network. From the current pattern of network deployment, this logical structure is emerging as the most natural architecture (Figure 2.2).

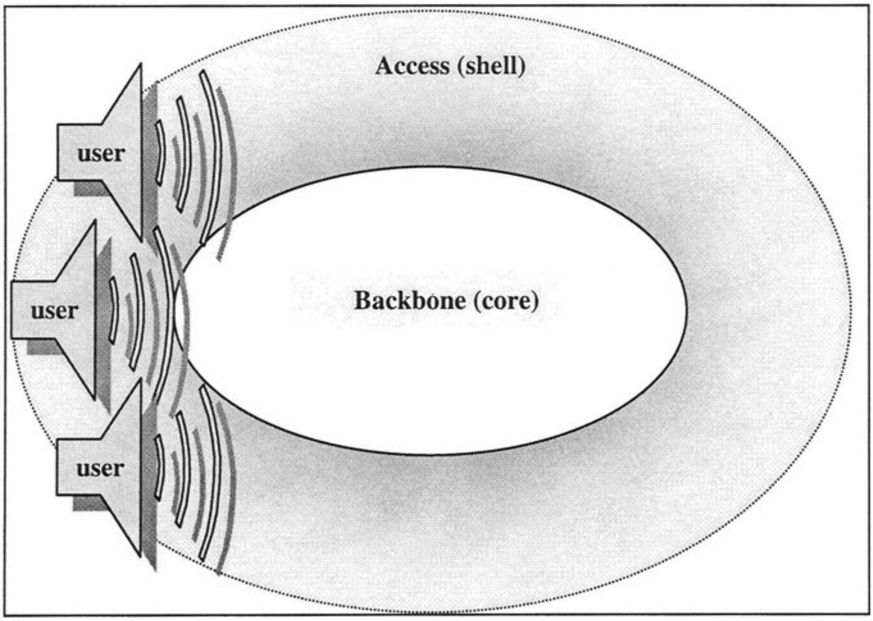


Figure 2.2 Basic structure of PervNet

Historically, it is driven by the architecture of immensely successful cellular voice service, which is popularly known as "last/first mile (hop) wireless" architecture. It may also be called as "wireless over wired" (WoW) [1], [3]. The last and the first miles of access have to be wireless because of the requirement to support mobility. The backbone may be either wired (say, optical) or wireless (say, satellite). Since optical transmission is the preferred technology for high speed high bandwidth backbone and single hop cellular is so far the common access technology, a popular implementation of this structure could be "cellular over optical". However, this does not imply that there are no other technologies for either backbone or access. It only indicates that these two technologies, namely optical and cellular, are the dominant ones from the point of both penetration rate and technological maturity. Since the bandwidth of wireless last hop is yet to match that of wired backbone, PervNet will prefer wired connection to wireless connection as far as possible. If there is no requirement of mobility at all, probably PervNet will not use wireless connection at any stage.

One may visualize that a combination of packet-based cellular WANs and low-power radio LANs will provide seamless PervNet connectivity over multi-hop, dynamic wireless networks in the future [4]. Consider for example, users in a train moving from London to Paris. The train may have single (or multiple) hubs that attach to PervNet via 3G cellular networks. Each compartment of the train may be a separate wireless LAN [3],[4], with each LAN separately connected to the central hub. Individual users may have laptops, which connect to the nearest LAN access point via wireless (802.11) LAN cards; finally, additional Bluetooth devices may connect to PervNet using the laptop as an intermediary. Consider what happens as the train moves to Bercelona and the hub attaches to a base station from a different provider with a different pool of global addresses. To ensure seamless connectivity to PervNet, the *entire network* that lies below the hub router, including the LAN access points, the laptops and the Bluetooth devices, must now obtain new (care-of) addresses that are part of the new cellular provider's pool. Clearly, it is not enough to simply configure individual mobile hosts, since the entire network (including intermediate routers) has exhibited aggregate mobility. We shall discuss more about the probable implementation strategies of this structure in following chapters.

2.2.2 Attributes

Before we can understand how to design PervNet, we should first explain what PervNet defines. Probably, the most distinctive two characteristics, that distinguish PervNet from other conventional types of networks, are its pervasiveness and heterogeneity. Above all, it is an internetwork, comprising all existing and forthcoming networks of the world, which is flexible and extensible to accommodate future applications. It should not be confused as a single global network. In reality, it would be an interoperable collection of networks that runs pervasive applications, with the scalability of supporting billions of users (static/mobile) and trillions of pervasive devices. It would be cost-effective for users in terms of services offered, and flexible and extensible to accommodate future applications.

The above considerations suggest that PervNet should accommodate the following desirable features:

a) Pervasiveness- the ability to be all-time and everywhere and to pervade all walks of life. The growth of PervNet appliances will fuel the deployment of 'home networks'. Consumers will clearly require plug-n-play functionality so that the appliances must be able to configure themselves automatically without requiring manual intervention.

b) Mobility- the ability to support global roaming. PervNet should know a pervasive device by a single name throughout the globe. It is exactly similar to the human behaviour, where a person need not change his/her name, if he/she travels to Europe from Asia or vice versa. Today terminal mobility is distinguished from personal mobility. In PervNet, stress will be more on personal mobility as pervasive devices will be easily available everywhere (like telephones or ATM counters).

c) Heterogeneity- the ability to deal with a large variety of network technologies that are not originally designed to work together. Examining the state of hardware technology today, it seems that the production of such processors and network interfaces is practical, if not yet commercially viable. The wide range of devices involved, from the smart can to the local supermarket's CPU cluster, will require a heterogeneous network, with the peripheral processors using different protocols (and physical media) to the Internet backbone. We assume that arbitrary connectivity is feasible, with the possible use of proxies or gateways as required. So there would not be any single PervNet standard that every component network has to abide by. Every constituent network can grow on its own; still they will be in the PervNet automatically (something similar to the fact that any LAN can join the Internet any moment).

d) Interoperability- the ability to accommodate and interwork with any technology and any application for effecting seamless integration across networks. This is closely related to the considerable and inherent heterogeneity of devices in a PervComp environment. Computing devices already cover a wide range of platforms, computing power, storage capacity, form factors, and user interfaces. We expect this heterogeneity to increase over time rather than decrease, as new classes of devices such as pads or car computers become widely used.

e) Quality of service (QoS)- the ability to guarantee certain performance measures (subjective or objective) for requested services transparently. QoS must be end-to-end and tuned to user intent. In most of the cases, context-awareness will drive the QoS requirement level. QoS need not be fixed throughout the period of interaction. It must be able to self-tune itself depending upon user perception, current network bandwidth, and other related parameters. Thus, it is pertaining to adaptation, transparency, and proactivity at the PervComp level.

f) Scalability- the ability to scale to all future expansion of users, devices and application needs. Not surprisingly, when most predictions of PervComp drastically underestimate the number of networked devices, current network architectures and their associated interface paradigms do not scale to this new world. For instance, even today, the primary concern in routing messages beyond a local domain is scalability. Now consider the case of PervNet. Both the traffic volume and the computational effort required to route messages in it must scale to support quadrillion of nodes, many of which will host multiple clients. Moreover, the ability to dynamically autoconfigure the entire network with addresses, and other network related parameters, such as default gateways, netmasks, DNS servers etc., in a scalable manner will be crucial to the implementation of PervNet. The dynamic nature makes the scale of autoconfiguration a key criterion.

g) Security- the ability to provide the required level of protection, privacy and trust to the users. It should be possible to prevent both the export and import of classes of messages in PervNet. Wherever the service crosses an enterprise boundary, some filtering of the traffic might be required in a similar fashion to firewalls used at the IP level. An administrator of a domain must be able to apply a filter at the domain boundary, protecting private information from dissemination and restricting the visibility of external events within the domain. While it should be possible to receive traffic from any connected server, not all domains will make all messages available.

h) Availability- the ability to be reliable enough and to provide service all time. Automatic failover to backup servers, load-sharing ability, robustness to individual and collective node mobility, and flexible configuration are the dominant requirements.

PervNet will be heterogeneous in many dimensions. At the backbone, there may be multiple constituent networks, such as the Internet, PSTN, satellite networks, packet radio networks and national WANs. At the access shell, there may be Ethernet LANs, wireless LANs, Bluetooth, ad hoc networks, CATV networks, wireless local loops and so on. We shall discuss about these network technologies in Chapters 3 and 4. These networks individually and collectively incorporate disparate transmission media, including UTP, STP, fibre optics, coaxial cables, microwave, radio, and infrared wireless. There will be a variety of devices with widely differing capabilities for context-awareness, display and processing, ranging from battery operated wireless PDAs to supercomputers. This heterogeneous infrastructure of PervNet will support a wide and a dynamic mix of applications varying from traditional applications (like telephony, e-mail) to typical pervasive applications (like service discovery, auto-registration).

2.3 PERVNET ARCHITECTURE

Although current network protocols are good for traditional (wireline) networks and offer many technology independent solutions, it must be remembered that they were not originally designed for even wireless networks, not to speak of PervNet. So their limitations will be exposed as we are moving to a PervNet like architecture. In fact, researchers strongly believe that the traditional protocols must be enhanced to a great extent in order to support PervNet. For instance, although IP supports DHCP, PPP and Mobile IP, still it cannot enable PervNet in its current form. It may so happen that, to make pervasive computing an economic reality, new solutions at several networking layers may be required. If functional enhancements are found to be insufficient, we may have to adopt brand new solutions at various layers.

Table 2.1 Proposed PervNet Architecture

No.	Name	Functions
5	Application Layer	Supports media translation and content adaptation
4	Service Layer	Combines the capabilities of multiple networked devices to collectively obtain "intelligent" services
3	Transport Layer	Manages end-to-end information distribution
2	Network Layer	Ensures connectivity and global roaming
1	Access Layer	Defines access schemes

Realizing that the PervComp vision will require significant additional research, beyond the recent advances in WAN, MAN and LAN (access) technologies, here we identify the desirable functionalities (to enable PervComp) for PervNet protocols and examine how the current architectures live up to these expectations. Sticking to the successful model of layered architecture, we first propose a 5-layer model (Table 2.1) for PervNet. Layer 1, called as *access layer*, defines medium access schemes and covers layers 1 and 2 of the traditional OSI model [1]. It more closely follows the lower 2 layers of TCP/IP suite [2] too. Layers 2 and 3 in PervNet resemble layers 3 and 4 in both OSI and TCP/IP structures. Layer 4, known as *service layer* in PervNet, is a new addition, reminding us of the layers 5 and 6 of OSI model. Finally, layer 5 is, as usual, the *application layer*. For the lower layers (namely layers 1 through 4), the functionalities are to be enhanced keeping the PervNet attributes in mind. The service layer is responsible for intelligence (or, smartness). At the service layer, for example, nodes must automatically access and combine the capabilities of multiple networked devices to collectively obtain "intelligent" services. For example, a home sprinkler controller should autonomously be able to query a subset of local temperature sensors in order to regulate its sprinkler activity. At the application layer, an area that has received considerable attention is media translation and content adaptation. Interface technologies (discussed in Chapter 5) normally handle these issues. We shall discuss the possible enhancements in the following sections.

2.4 MANAGING PERVASIVENESS

The prime aspect of pervasiveness relates to addressing and routing, which are handled by the layer 3, namely the network layer. Though mobile ad-hoc networks [3] typically focuses on developing dynamic host-based routing protocols to ensure continuous connectivity, such host-based protocols and a flat routing architecture are appropriate for relatively small-sized ad hoc networks. In contrast to such a scenario, PervNet is a much larger network, where a scalable addressing (such as hierarchical) is essential, and where the auto-configuration process not only enables local connection but also provides global connectivity to PervNet.

2.4.1 Autoconfiguration

A major issue in pervasiveness is obtaining configuration information, such as node addresses (say, IP address) and addresses of key servers (such as DNS), automatically and dynamically. For instance, in order to provide pervasive devices with globally reachable (say, IPv6) addresses [3], we must develop automated mechanisms that distribute addresses (may be from a pool); PervNet providers simply cannot afford to manually configure each individual network node! Hence, nodes attached to PervNet must obtain its own address as well as addresses of key resource servers, before they can establish connections for communication. Existing configuration protocols such as PPP [5], DHCP [6], and Mobile IP [7] (with Foreign Agents) can configure hosts (see Chapter 7 also). However, given that many of these nodes may act as routers, PervNet requires that autoconfiguration must be extended to configure routers and even large unmanaged dynamic (ad hoc) networks.

Auto-configuration capability is important not just from a practical network management standpoint, but also to allow networked devices to automatically discover and exchange capability information. For example, addressing is equally important for successfully routing in traditional data dissemination paradigm, where the originator of the message must know where it is to be sent (directed communication). The problem with requiring knowledge of the destination is that sometimes you do not have it. Resolving addresses for directed communication has absorbed a great deal of distributed systems research over the past decade and has led to the development of numerous methods for obtaining addresses:

- use standardized names, a name server, and a reserved address for local name servers, or
- use LAN segment broadcast or a reserved multicast address to find named objects, or
- use a yellow pages service at a reserved address, and select one of the available services in the required class by its advertised properties, or
- perform a multicast request to a reserved group, and have all services listen to that group and respond if they can provide the requested function.

Protocols such as PPP [5], designed for serial links, and DHCP [6], designed for broadcast LANs, for example, operate in a client-server mode. The client (host) dynamically requests an address and other configuration parameters from a preconfigured server. This server preconfiguration is geared towards environments where network dynamicity is restricted to one hop at the network edge. Newer approaches for host auto-configuration include the IPv6 stateless auto-configuration [8] mechanism and the Dynamic Registration and Configuration Protocol (DRCP) [9], an extended version of DHCP that provides rapid host configuration, especially over wireless links. This list is only superficially representative, and yet none of these approaches really solve the problem. Each of them merely shifts the required knowledge to a level of indirection, without addressing the basic issue: *that the destination address must be known.* So they are not suitable for PervNet, which demands for developing protocols that allow entire networks, possibly connected in a dynamic topology, to form self-organizing hierarchies. In contrast to our goal of network auto-configuration, research efforts in the Internet community have so far focused on the more limited objective of auto-configuring hosts and small networks (interested readers can refer to Chapter 6 for more details). Relatively little work, however, exists on mechanisms for rapid and robust auto-configuration of large dynamic networks, which is the requirement for PervNet.

2.4.2 Registration

In PervNet environment, ubiquitous access to network resources will be a pressing need, and this requirement is distinct from the problem of assuring continuous connectivity for mobile hosts and users. Hence, it is necessary to have a uniform registration protocol, independent of mobility and configuration mechanisms, to provide authorized access to PervNet resources and services. This will allow users to register even at a foreign sub-network, irrespective of the choice of configuration and binding protocols. Also, PervNet must have mechanisms that allow network nodes to authenticate a user and to determine his/her service requirements (say QoS needs). At present, AAA interface in PPP and mobile IP provides the requisite functionality for wired and wireless environments, respectively, which can be ported to PervNet without much fuss. When the users are mobile, mobile IP can be used (with its newly defined AAA interface). When the users are accessing over serial (e.g., telephone) lines, then PPP can be used (with its well defined AAA interface). However, since AAA is a Network-to-Network Interface (NNI), what is missing is a common user-network interface (UNI) for registration. An approach based on the Basic User Registration Protocol (BURP) with its interface to AAA protocols, such as DIAMETER, and where DHCP is used as configuration protocol is described in [9]. Using BURP as user registration protocol in PervComp, network providers will have better information and control of network usage. It is envisioned that BURP will be easy to implement and deploy on current operating systems. Being an application layer protocol, its implementation can be done in user space and it requires no changes to the TCP/IP stack. It is assumed that DHCP is capable of offering the BURP.

2.4.3 Routing

Till today, for traditional networks, we have been using *directed* communication models: the destination of the message is specified at the time it is sent (in the case of multicast, this specification is not a single address, but a group or channel upon which the senders and receivers have previously agreed). However, in a system where we seriously expect quadrillions of computers, and several orders of magnitude more active end-points (or objects), and where the set of these relevant information is in constant flux to an individual at rates of up to hundreds per second, requiring that the sender of a message always specify its destination does not appear feasible. Also, simply forwarding all traffic from a local domain onto a global PervNet bus is infeasible because of scalability problem. Ideally, only those messages that exactly match the requirements of one or more subscribers, somewhere on PervNet, should be sent on. In effect, the backbone should subscribe to a set of messages from a local domain.

Given that this is the case, the current routing paradigms could, not by simple extension, support the PervComp scenario. So, what we may look for is content-based undirected routing (sounds similar to content-addressable memory!). *Undirected communication* is that where the sender of the messages does not specify their destination. This works by using a "pull" style, content-based selection of messages. Content-based routing is a fundamentally different paradigm for interaction between networked objects. By removing the necessity for producers to direct messages, we gain enormous flexibility in system architecture and scalability over traditional communication systems allowing us to provide an interactive environment for PervComp. Undirected communication facilitates systems that are more easily extended, simpler to componentize, and contain a clearer mapping to real world interactions between objects.

To avoid the perils of perception altogether in a PervNet, one can assume that network or data connectivity is equivalent to co-location [4]. This implies that if two devices can communicate directly (by RF, IR or other "local" transmission method), they are co-located. However, RF transmission (not to mention physical network protocols) can easily span rooms, floors or even buildings. Without some more precise model of geometry, this type of assumption will result in an excessively large set of potentially available devices, many of which may not actually be available or usable for any particular task due to the vagaries of the transmission method.

2.5 MOBILITY MANAGEMENT

Supporting user mobility and terminal mobility is a key requirement for the PervComp environment. As the pervasive environment is all-inclusive, the user requirements on connectivity will be diverse. To ensure pervasive connectivity, PervNet must accommodate a mobility management architecture that provides ubiquitous connectivity to an extremely large number of mobile/static nodes over a variety of link technologies. Moreover, as users and nodes exhibit dynamic mobility, PervNet must ensure that they continue to gain access to network resources and services. While some applications, such as Web access, will not need users to be locatable or even require continuous connectivity, other important applications, such as Voice-over-IP (VoIP), tracking objects/users, modeling environment, not only require other users to be able to locate them, but also expect seamless session (continuous connectivity). An IP-based mobility solution offers this desired independence of the access technology specific mobility solutions. However, current IP-based approaches, such as the standard mobile IP [10] approach, are designed for environments where only a small fraction of the hosts exhibit mobility. Moreover, mobile IP and other existing protocols are not enough for real-time pervasive applications since no uniform fast handoff and paging mechanisms are available.

So we need a versatile mobility management scheme that can handle a good amount as well as degree of pervasive mobility. Also, the pervasive mobility management solution must scale with significantly larger number of mobile nodes. Additionally, the ability to support optional features, such as fast handoff and paging, which may be critical for certain mixes of application and access devices, is essential. For example, interactive voice applications (such as VoIP) will require low bandwidth but tight delay and handoff bounds, while notification-type applications may require low handoff loss and network paging support to minimize the power consumption.

A closer look at the current techniques for ensuring pervasive connectivity will reveal that mobility management essentially consists of three distinct operations:

- User/Node Configuration
- User/Node Registration
- Dynamic/Global Binding

It is interesting to observe that current IP-based solutions, such as Mobile IP, often integrate all three functionalities, leading to a non-modular architectural design and making it harder to reuse existing protocols in different networking scenarios. Thus, in the foreign agent mode of Mobile IP, an MN is configured in the foreign network by obtaining a care-of address from the FA. Registration in Mobile IP consists of negotiating lifetimes and authentication information with the FA, as well as the HA. Dynamic binding in Mobile IP is achieved by informing the HA (or the CNs) of the current Care-of-Address (CoA), so that packets can be re-routed to the MN's current point of attachment. A SIP-based mobility solution, while using different protocols and message formats, also follows a similar approach to ensure continuous reachability. Such integrated solution allows an MN to achieve continuous and roaming reachability, since the location of the MN is available at centralized databases (HA or SIP [10] Server).

Although Mobile IP [7] recently joins forces with Authentication, Authorization and Accounting (AAA) protocols (such as DIAMETER or RADIUS), we, however, believe that Mobile IP or SIP-based continuous reachability is not always required or desirable. A different form of untethered and roaming access to network resources will become equally important in future PervNet scenarios, such as access to airports, shopping malls and sports stadiums etc. In these scenarios, users simply access (pull) network services using local LANs and borrowed nodes; configuration and registration are thus become important. While configuration protocols like DHCP [6] or DRCP [9], provide a valid address in the network; no user authentication or authorization is involved in this process. Internet Service providers (ISPs) currently use RADIUS over PPP [5] for authentication and authorization to their dial-up users. It is very unlikely that connection to Internet or home ISPs in airports, shopping malls or sports complex will be via telephone lines. The obvious choice will be wireless LAN and in such a scenario, a User Network Interface (UNI) registration protocol is very much essential for network access and control.

2.6 SERVICE DISCOVERY

The widespread deployment of inexpensive communications technology, computational resources in the PervNet infrastructure, and network-enabled pervasive devices pose an interesting problem for PervComp environment: how to locate a particular network service (or device) out of hundreds of thousands of accessible services (and devices). This is known as service discovery problem, and there must be another service to provide this discovery service. Moreover, this service discovery service (SDS) has to provide a highly available, fault tolerant, incrementally scalable service for locating services in PervNet. In SDS, security will be a core component and, where necessary, communications are both encrypted and authenticated. Service providers will use the SDS to advertise descriptions of available or already running services, while clients use the SDS to compose complex queries for locating these services. Service descriptions and queries may use some standard language (such as XML) to encode such factors as cost, performance, location, and device- or service sp ecific capabilities. Furthermore, the SDS may use a hybrid access control list and capability system to control access to service information.

Several interesting approaches to automated capability and service discovery have been recently proposed. For example, the Service Discovery Protocol (SDP) [11] has been standardized in the Bluetooth architecture as a client-server approach to exchange node capabilities in local short-range networks. However, SDP is not designed for exchanging configuration information, nor does it provide mechanisms for managing dynamic node mobility. The Jini architecture [12] provides a Java-based solution for devices connected in an ad-hoc configuration to exchange capabilities by moving Java objects between Java Virtual Machines. Another example is Service Manager (http: // www.webenterprisesuite.com / service_manager/), which is a catalog toolkit that is Open GIS Consortium (OGC)-compliant and provides discovery, access, harvesting and maintenance of web-based services metadata. The Service Manager architecture has been specifically designed to be deployed in a multi-tier arrangement of clients and servers and discovery of services is provided through Service Manager Client Java classes that enable a client to locate service metadata quickly and effectively. The application also has a metadata harvest process that will automatically ingest service metadata from OGC-compliant map servers.

2.7 DISCONNECTED OPERATION

We have already encountered this problem in MobiComp. But, in PervComp, the main idea behind disconnected operation is to force developers to build applications that better cope with a highly dynamic environment of PervNet, while also providing primitives that make it easier to implement applications. This is important to ensure transparent access to remote resources in a PervNet environment where disconnection is a common phenomenon.

By building on distributed file systems or remote procedure call packages, many existing distributed systems mask remote resources as local resources. This transparency certainly simplifies application development. From the programmer's viewpoint, accessing a remote resource is as simple as a local operation. However, this comes at a cost in failure resilience and service availability. Network connections and remote servers may fail. Some services may not be available at all in a given environment. As a result, if a remote service is inaccessible or unavailable, distributed applications cannot provide their services, because they were written without the expectation of change. We believe that this transparency is misleading in a PervComp environment, because it encourages a programming style in which a failure or the unavailability of a resource is viewed as an extreme case. But in an environment where tens of thousands of devices and services come and go, the unavailability of some resource may be the common (or at least frequent) case. We are thus advocating a programming style that forces applications to explicitly acquire all resources, be they local or remote, and to be prepared to reacquire them or equivalent resources at any time.

It is always better to have support for saving and restoring application *checkpoints* and for *migrating* applications and their data between nodes. Checkpointing and migration are useful primitives for building failure resilient applications and for improving performance in a distributed system. Furthermore, migration is attractive for applications that follow a user as he/she moves through the physical world. Checkpointing and migration affect an environment and its contents, including all nested environments. Checkpointing captures the execution state of all components in an environment tree and saves that state in form of a tuple, making it possible to later restore the saved state. Migration moves an environment tree, including all components and stored tuples, from one device to another. Since applications already need to be able to dynamically acquire resources they need, both checkpointing and migration eschew transparency and are limited to the resources contained in the environment tree being checkpointed or migrate.

2.8 PROPOSED SOLUTIONS

Here we will briefly discuss the present state-of-art in PervNet research at a glance. This is not an exhaustive list. Specific topics will be described at length in the following chapters.

2.8.1 It's Time to PIP

Most of the recent works [9] have attempted to tackle pervasiveness at the network layer. So, quite naturally, their focus is primarily on IP. It is true that network layer (and IP in particular) will play a major role in PervNet because, to provide link-layer independent solutions, PervNet will desire both pervasiveness and mobility management functions at the network (IP) layer. In a sense, what we are looking for exactly is a pervasive version of IP i.e., PIP (*Pervasive IP*) in short. PIP also supports the service requirements of diverse applications and devices, which are important for providing PervNet connectivity. We shall discuss about IP-related solutions in Chapter 6, and there it will be clear how difficult is the proposition to obtain a model for PIP.

2.8.2 Dynamic Configuration

One approach, based on the Dynamic Configuration Distribution Protocol (DCDP), is described in [9]. DCDP is a spanning tree based configuration distribution protocol that enables large dynamic networks to rapidly auto-configure an addressing hierarchy and subsequently distribute service-specific information without any manual intervention. Network nodes, which are responsible for advertising and discovering additional configuration and capability information, can also use its own hierarchical distribution mechanism. DCDP is actually an extension of the initial version of the Dynamic Address Allocation Protocol (DAAP) [9], which used a binary-splitting scheme to distribute address pools over an extended multi-hop network. After realizing the flexibility of DAAP's top-down address distribution mechanism, they have recently extended and modified it to define DCDP as an all-purpose configuration dissemination solution.

2.8.3 Auto-Registration

An application layer Basic User Registration Protocol (BURP) [9] is a potential solution to this problem. The motivation behind BURP is to provide a standardized UNI to achieve seamless registration, wherein IP connectivity services are offered using configuration protocols such as DHCP, DRCP or IPv6 stateless autoconfiguration [8]. Unlike Mobile IP-AAA registration, BURP is an application layer protocol and it interacts with a local *Registration Agent* (RA). The location or address of the RA server is assumed to be known by the client during configuration process.

The initial idea of BURP was presented in IETF-48 (AAA-WG) held in Pittsburgh, July 2000. Since the design and specification of BURP is not yet complete, we will discuss following important features and protocol message flow. BURP is independent from the configuration protocols. It is a client-server application layer protocol. All BURP clients implement registration and deregistration schemes. It works for both IPv4 and IPv6. User interacts only with a local RA, which may reside on any node in the PervNet domain. It interacts with routers/policers to limit packets forwarding based on a user's Service Level Specification (may also interwork with standard policy protocols).

Registration agent may interface to the backend AAA server such as DIAMETER or RADIUS. BURP has flexible extension mechanism and also extensible to support various authentication schemes. It is capable of supporting vendor or organization specific extensions. RA offers protection against reply and man in the middle attacks. BURP supports challenge/response authentication whenever necessary. It has the ability to quickly detect whether the terminal has left the access network or not.

2.8.4 Dynamic Mobility Management

A Dynamic Mobility Agent (DMA)- based approach to mobility management is presented in [9] to discuss how the architecture provides a scalable solution for supporting seamless connectivity for a wide range of application classes. DMA architecture provides a stable point of attachment within a network and includes support for features such as QoS assurances, fast handoff and paging [9]. It is based on an extension of the conventional Mobile IP approach and uses multiple agents, called *Mobility Agents* (MAs) to distribute the mobility load in a single domain.

Additionally, by using a separate Intra-Domain Mobility Management Protocol (IDMP) [13] for managing mobility within a domain, the architecture supports the use of multiple alternative global binding protocols (such as Mobile IP [7] or SIP [10])) for maintaining global reachability. Most importantly, this approach can leverage existing IP-layer functionality to provide support for features, like fast handoffs, paging and QoS guarantees, that are important for providing mobility support to a diverse application set.

2.8.5 Content Based Routing

A content-based message routing system is under development at Elvin project [14]. It provides undirected communication, using content-based subscriptions to route self-describing messages. It can easily, if inefficiently, emulate directed communication, leading some to propose it as a universal communication model. It can be used in conjunction with directed forms of communication, selecting the model most appropriate for the task at hand. For content-based addressing to work, message *consumers* (destinations) must have a way to specify that they want to receive a certain class of messages. This information is then used by the infrastructure to route the appropriate messages to the consumer. For the consumer to select a message from a producer (or source), it must somehow describe the message it is to receive. If this description is reduced to its simplest form, it effectively becomes a multicast address: a single, unique attribute used to identify a class of messages. But using a single, unique attribute to identify messages offers no advantage over directed communication.

While ultimately the consumer must share some knowledge with the producer(s), this knowledge can be structured to provide a flexible means of identifying pertinent messages by specifying selection criteria expressed in terms of the message's contents. These specifications may be called *templates* and they describe the number, type and order of the message's attributes. The value of a particular attribute can be fixed by providing a value, or is otherwise constrained only to the required data type.

In essence, Elvin routes undirected, dynamically typed messages between producers and consumers. Messages consist of a set of named attributes of simple data types. Consumers subscribe to a class of events using a boolean subscription expression. Elvin can be described as a pure notification service Notification services also provide a degree of undirected communication. In some propositions, the directedness of notification forms the *naming model*, where classes of events are named using either a structured name, or a property-based name. The degree of direction extends from a multicast address (very directed), through a filter-able structured name, to a property-based query (least directed). Producers push messages to the service, which in turn delivers them asynchronously to consumers. When a message is received at the service from a producer, it is compared to the registered subscription expressions for all consumers and forwarded to those whose expressions it satisfies. Messages can be sent without pre-registration of message types and subscriptions can be added, modified, or deleted at whim. The system is implemented as a server daemon that provides the subscription registry and evaluation engine. Client libraries map the wire protocol to programming languages.

This mechanism will scale to an almost indefinite number of consumers. Servers will have a *hand-over* facility, allowing a single, advertised server to balance the client load within the cluster. This facility can also be used to perform handover of clients for graceful shutdown. For ease of administration, connections between servers within a local domain are not subject to topology constraints. To ensure messages are not duplicated, regardless of the inter-server links, each message is tagged with sufficient information to detect duplicates, which are then discarded. Links between servers are unidirectional, and have optional filters to control message propagation.

2.9 SUMMARY

Every time, everywhere networking technology is available today and location awareness as a part of context awareness promises new applications. However, is it possible to combine these two and build a location-aware infrastructure without extra locating system on top of PervNet technology? To answer this question, this chapter has presented a possible architecture of PervNet that is coming up from the existing technologies. The technology already exists. However, current protocols do not meet the requirements (e.g., persistent network access). Nevertheless, projects try to use, for instance, wireless LANs to provide large scale, every time, everywhere network access. The bay area of San Francisco (see www.bawug.org) is a good example for such a project. Recently, Sydney also started such an effort (see www.sydneywireless.com/db2). Other hot spots are Starbucks coffee shops, airports, universities, and hotels. In such places, users can seamlessly connect to the Internet via a wireless LAN. Although different wireless LAN standards exist, most such network base on the IEEE 802.11b. In a word, PervNet is feasible today and pervasive location-awareness is feasible today. Furthermore, it is possible to combine these two and build location-aware services on top of pervasive networking technology. However, this is limited to reactive services only as it is yet to build proactive services. Nevertheless, as especially proactive services will play an important role in the near future and allow a much larger variety of services than just reactive services, we expect much research activity in that area in near future.

REFERENCES

[1] Warland J. and Varaiya P, *High Performance Communication Networks*, 2nd Edition, Morgan Kaufmann, 2000.

[2] Comer D. E., *Internetworking with TCP/IP*, vol. 1,2,3, 4th Edition, Addison Wesley, 2000.

[3] Linnartz J-P (Ed.), *Wireless Communication*, the interactive multimedia CD ROM, Kluwer Academic, 1st Edition, 2001.

[4] Special inaugural issue on *Reaching for Weiser's Vision*, IEEE Pervasive Computing, Vol. 1, No. 1, Jan-Mar 2002.

[5] Simpson W., "The Point to Point Protocol (PPP)", Internet STD 51, July 1994.

[6] Droms R., "Dynamic Host Configuration Protocol", RFC 2131, IETF, March 1997.

[7] Perkins C., "IP Mobility Support", RFC 2002, IETF, October 1996.

[8] Thomson S. and Narten T., "IPv6 Stateless Address Autoconfiguration", RFC 2462, IETF, December 1998.

[9] McAuley A, Das S., Baba S. and Shobatake Y., "Dynamic Registration and Configuration Protocol", draft-itsumo-drcp-00.txt, IETF, July 2000, Work in Progress.

[10] Wedlund E. and Schulzrinne H., "Mobility support using SIP," Proceedings of Second ACM International Workshop on Wireless Mobile Multimedia, ACM/IEEE, August 1999.

[11] Bluetooth SIG, "Service Discovery Protocol Release 1.0", July 1999, http://www.bluetooth.com/developer/specification/profile 10 b.pdf

[12] Arnold K., Sullivan B. et al, "The Jini Specification", ISBN 020-1616343, Addison-Wesley, June 1999.

[13] Misra A., Das S., McAuley A., Dutta A. and Das S. K., "IDMP: An Intra-Domain Mobility Management Protocol using Mobility Agents", draft-mobileip-misra-idmp-00.txt, IETF, July 2000, Work in Progress.

[14] http://www.dstc.edu.au/Elvin/

Chapter 3

Backbone Technology

Chapter 2 has discussed the architecture of PervNet where the backbone is depicted as the core of the network model. In fact, backbone constitutes the foundation technology of PervComp, which is to be used in any pervasive application for transmitting multimedia information containing plaintext, hypertext, audio, images, video, and data. In PervNet, devices communicate over an access network that connects to a core network–commonly known as a network backbone. For example, a pervasive device may be connected to a wired/wireless local area network (LAN), which is connected to other networks either directly or through a backbone of wide area network (WAN). It may so happen that data need to be transferred from one network to another, or from one network segment to another. For data to be transmitted across networks usually requires an interface device, such as a bridge, gateway or router. An interconnection of networks is commonly known as an internetwor (or internet in short). Each part of an internet is a subnetwork (or subnet in short). Internetworking is becoming more important especially as more devices are becoming pervasive and they need to intercommunicate with each other. The Internet is a special kind of internet (that uses TCP/IP suite), which is growing at an enormous speed to be the kernel of the backbone for PervNet. This chapter gives an introduction to the common technologies being used currently for backbone networks, including the Internet that is discussed at length in Chapter 6.

3.1 INTRODUCTION

Since PervNet is a heterogeneous network, multiple technologies will be accommodated within it. There may be Ethernet, FDDI, ATM, TCP/IP, WDM [1]-[3] and so on. Much alike the Internet, its growth will be ad-hoc through internetworking devices wherever necessary. Typically, it will be centred around the Internet because it is already there, and it has pervaded the globe to a large extent. So PervNet may be visualized as a superset of the Internet by including all existing (many of which are non-TCP/IP networks) as well as upcoming networks (most of which are TCP/IP networks) to it. For instance, it will contain the NSFNET's T1 backbone in USA (Figure 3.1), which is an essential part of the Internet backbone already. Similarly, all nation-wide backbones in different countries will automatically be added to PervNet backbone.

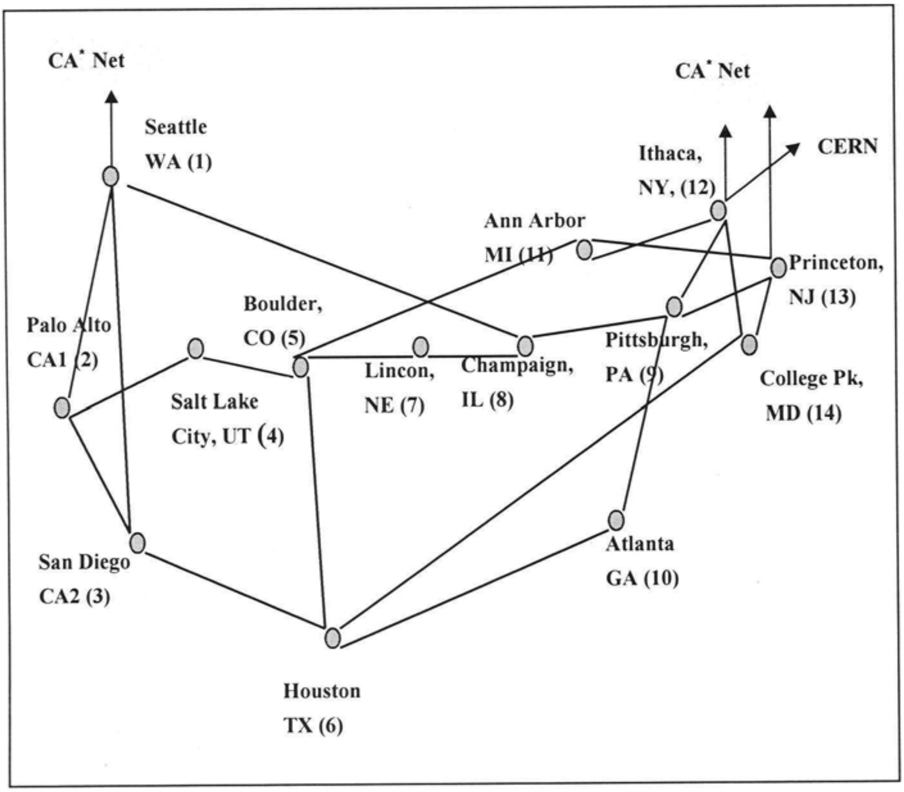


Figure 3.1 NSFNET's T1 backbone

It is to be noted here that local backbone networking technologies, such as Ethernet, Token Ring and FDDI [1] provide a data link layer function, that is, they allow a reliable connection between one node and another on the same network. They do not provide for internetworking, where data can be transferred from one backbone network to another or one backbone network segment to another. For data to be transmitted across networks requires protocols like TCP/IP containing an addressing scheme which is read by a bridge, gateway or router, leading to the formation of an internet.

Usually, different technologies are found to be cost-effective at different levels of backbone development. Also, with the advent of new technologies, network architectures and protocols are changing constantly. Earlier where microwave or satellite communication was used, optical fibre is being used recently. A few years back optical fibre was so costly that nobody can think of laying it in LANs. But it is so commonplace now that even in local loops fibre is being used (e.g., FTTH: fibre to the home [4]). As it seems, optical networks will constitute a major portion of the PervNet backbone (if not access). In optical networks, wavelength division multiplexing (WDM) [2],[3] and dense WDM (DWDM) [4] technologies are maturing very fast to replace other technologies. This is why the emphasis of this chapter will obviously be on WDM/DWDM. However, before delving into WDM, we will discuss other prevalent technologies in brief for the sake of continuity.

The performance of a network backbone is extremely important as the perception of many users on the network depend on it. If the traffic is too heavy, or if it develops a fault, then it affects the performance of the whole network. In PervNet, the number of devices will be a few orders of magnitude more than what we see today. So backbone technology is even more important in the context of PervComp.

3.2 ELECTRICAL BACKBONE NETWORKS

Historically, electrical networks are temporally older than optical networks. So we begin with them.

3.2.1 Fast Ethernet

Ethernet [1] is the most widely used networking technology used in LAN backbones. In its standard form, Ethernet allows a bit rate of 10 Mbps only using either coaxial or twisted-pair (Category 5, or CAT 5 in short) cables. Since it defines only the lower two layers, it cannot make a network on its own; it needs some other protocol, such as TCP/IP, to allow nodes to communicate. Even though Ethernet does not cope well with heavy traffic, it has many advantages: cheap to install, components are easily available, well-proven technology, fairly scalable architecture, and supported by most software and hardware systems. This is why it has become so much pervasive in LAN domain. However, scalability is still a big problem with it. Standard 10 Mbps Ethernet does not perform well when many devices/users are running multimedia applications, which will be a common phenomenon in PervNet. There Fast Ethernet [1] systems that minimize the problems of contention and increase the bit rate to 100 Mbps will be more appropriate in the sense that it gives at least 10 times the performance of standard Ethernet.

So, for small area backbone in PervNet, Fast Ethernet (100BASE-TX or 100VG-Any LAN) will be popular. The IEEE has defined standards for both of them, IEEE 802.3u for Fast Ethernet and 802.12 for 100VG-AnyLAN, which are supported by many manufacturers [1]. On a Fast Ethernet network with twisted-pair copper cables, the maximum distance is 100 m, and, for a fiber-optic link it is 400 m. Fast Ethernet, or 100BASE-T, is simply 10BASE-T running at 10 times the bit rate. Since 100BASE-TX standards are compatible with 10BASE-TX networks, the fast Ethernet allows both 10 Mbps and 100 Mbps bit rates on the line. This makes upgrading simple, as the only additions to the network are dual-speed interface adapters. Nodes with the 100 Mbps capabilities can communicate at 100 Mbps, but they can also communicate with slower nodes, at 10 Mbps. Therefore, fast Ethernet is a natural progression from standard Ethernet and thus allows existing Ethernet networks to be easily upgraded. New standards relating to 100 Mbps Ethernet are: a) 100BASE-TX (twisted-pair)– which uses 100 Mbps over two pairs of Cat-5 UTP cable or two pairs of Type 1 STP cable, b) 100BASE-T4 (twisted-pair)– which is the physical layer standard for 100 Mbps bit rate over Cat-3, Cat-4 or Cat-5 UTP, c) 100VG-AnyLAN (twisted-pair)– which uses 100 Mbps over two pairs of Cat-5 UTP cable or two pairs of Type 1 STP cable, and d) 100BASE-FX (fiber-optic cable)– which is the physical layer standard for 100 Mbps bit rate over fiber-optic cables.

3.2.2 Gigabit Ethernet

Unfortunately, even with fast Ethernet, nodes contend for the network bandwidth, reducing the network efficiency when there are high traffic rates (as will happen in PervNet). Also, as it uses collision detect, the maximum segment length is limited by the amount of time for the farthest nodes on a network to properly detect collisions. So, efforts are on to raise the bit rate of Ethernet further from 100 Mbps. Fast Ethernet has been upgraded to 1000 Mbps (Gigabit Ethernet) on UTP cables. Gigabit Ethernet [1], specified as 1000BASE-T, operates today over Category 5 and Category 5E (enhanced) cabling. 1000BASE-T can also operate on the cabling specified to the current drafts of Category 6 (Draft 5) and Category 7. When the ratification of 1000BASE-T (IEEE 802.3 Ethernet Standard for Gigabit Ethernet on Category 5 copper) was done in June 1999, migration of the installed base of Category 5 to higher speed Ethernet was the primary concern for network managers because they wanted to future proof their network infrastructures (very important for PervNet growth). While 1000BASE-T was specified to run over Category 6 cabling, most of the cabling installed that time was Category 5. So the IEEE has to ensure the operation of 1000BASE-T Standard over the Category 5 cabling systems installed according to the specifications of ANSI/TIA/EIA-568A (1995). The primary goal of the IEEE 1000BASE-T Task Force, responsible for the development of the 1000BASE-T standard, was to support the legacy Category 5 cabling so that there should be no need to replace existing Category 5 cabling to use 1000BASE-T. According to the Task Force, any link that is currently using 100BASE-TX should easily support 1000BASE-T. This is certainly a good news for PervNet.

1000BASE-T also uses a symbol rate of 125 Mbaud, but it uses all four pairs for the link and a more sophisticated five-level coding scheme. In addition, 1000BASE-T sends and receives simultaneously on each pair. Combining 5-level coding and 4 pairs allows 1000BASE-T to send one byte in parallel at each signal pulse. Thus, [4 (pairs) * 125 Msymbols/second * 2 bits/symbol] = 1Gbps. Of course, it is not quite this simple. In addition to moving the symbols across the link, 1000BASE-T must also deal with the effects of insertion loss and link-induced interference caused by echo and crosstalk. Topology rules for 1000BASE-T should be the same as those used for 100BASE-TX. Category 5 link lengths are limited to 100 meters by the TIA/EIA-568-A cabling standard. 1000BASE-T is specified for operation over those link lengths, as is 100BASE-TX. Half-duplex collision domains are similar to 100BASE-TX; however, each half duplex collision domain can support only one half-duplex repeater.

Reports are coming that 10 Gbps has been successfully tried in the laboratory. These are certainly good news for PervNet that always looks for more speed and more bandwidth. The 10 Gigabit Ethernet Alliance (10GEA: http://www.10gea.org/) has been organized to facilitate and accelerate the introduction of 10 Gigabit Ethernet into the networking market. It was founded by networking industry leaders, such as 3Com, Cisco Systems, Extreme Networks, Intel, Nortel Networks, Sun Microsystems, and World Wide Packets. Additionally, the Alliance will support the activities of IEEE 802.3 Ethernet committee, foster the development of the 802.3ae (10 Gigabit Ethernet) standard, and promote interoperability among 10 Gigabit Ethernet products. Recently, the IEEE Standards Association (IEEE-SA) unanimously approved the IEEE 802.3ae specification for 10 Gigabit Ethernet as an IEEE standard.

Positioned as a high-speed, unifying technology for networking applications in LANs, MANs, and WANs, 10 Gigabit Ethernet will provide simple, high bandwidth at relatively low cost. In LAN backbones, 10 Gigabit Ethernet will enable organizations to scale their packet-based networks from 10 Mbps to 10,000 Mbps, thereby leveraging their investments in Ethernet.

In MAN and WAN applications, 10 Gigabit Ethernet will enable service providers and others to create extremely high-speed longer distance Ethernet links at very competitive cost. All theses will lead to a successful implementation of PervNet backbone in coming years. Specific information about the IEEE P802.3ae can be found in IEEE 802 web site at http://www.ieee802.org.

3.3 OPTICAL BACKBONE NETWORKS

One of the greatest revolutions in data communications is the usage of light waves to transmit digital pulses through fiber optic cables [3]. A light carrying system has an almost unlimited information capacity. Moreover, fiber cables are more resistive to environmental extremes. They operate over a larger temperature variation than copper cables and are affected less by corrosive liquids and gases. Fiber cables are safer and easier to install and maintain (as glass and plastic) because they have no electrical currents or voltages associated with them. Optical fibers can be used around volatile liquids and gases without worrying about the risk of explosions or fires. Fiber cables are more electrically secure than their copper counterparts and are virtually impossible to tap into without users knowing about it.

Fiber optic cables are also smaller and more lightweight than copper cables. They have a much higher specification than copper cables and allow extremely long connections. Single-mode fibers have a narrow core, such as 10 μm for the core and 125 μm for the cladding (known as 10/125 micron cable) [3]. This type allows light to enter only at a single angle. Multimode fiber has a relatively thick core, such as 62.5μm for the core and 125 μm for the cladding (known as 62.5/125 micron cable). Multi-mode cable reflects light rays at many angles. The disadvantage of these multiple propagation paths is that it can cause the light pulses to spread out and thus limit the rate at which data is accurately received. Thus, single-mode fibers have a higher bandwidth than multimode fibers and allow longer interconnection distances [1]-[3].

Fiber systems are immune from cross-talk between cables caused by magnetic induction. Glass fibers are non-conductors of electricity and therefore do not have a magnetic field associated with them. Fiber cables do not suffer from static interference caused by lightning, electric motors, fluorescent lights, and other electrical noise sources. This immunity is because fibers are non-conductors of electricity. This is exactly what PervComp environment demands for. Fiber systems have greater electrical isolation, thereby allowing equipment greater protection from damage due to external sources. For example, if a receiver is hit by lightning pulse them it may damage the opto-receiver, but a high voltage pulse cannot travel along the optical cable and damage sensitive equipment at the source end [1],[3]. Fiber cables do not radiate energy, and, therefore, cannot cause interference with other communications systems. This characteristic makes fiber systems ideal for PervNet applications, where the effect of electromagnetic interference may have a devastating effect on sensor communication systems.

Fiber systems have a greater capacity due to the inherently larger bandwidths available with optical frequencies. Theoretically, it has more than 200000 times the capacity of a satellite TV system. This makes it appropriate for PervNet backbone where nobody knows what is the required limit of bandwidth. Thus, fiber optic technology holds out the promise of catering to the ever-increasing demand for bandwidth intensive end-user applications of PervComp. However, today's optical network infrastructures are best suited for predictable, connection-oriented voice traffic, not bursty high-bandwidth, dynamic transport of multi-media services. But PervNet architecture is now evolving optical networks [4] to acquire the capability to better accommodate these more advanced services. For example, reduced provisioning time is a prerequisite of emerging optical networks. Software in optical switches should support dynamic provisioning requirements without manual intervention. Only then, PervComp services may be offered at an even lower price while maintaining the traditional management features so the customer only pays for the bandwidth and time used. Emerging standards will also make possible for edge devices to automatically request instant bandwidth from the core.

3.3.1 FDDI

Fibre Distributed Data Interface (FDDI) [1] backbone is a fibre-based ring topology and is very common for backbones in metropolitan area networks (MANs). It has a high bit rate operating at 100 Mbps. To overcome the problems of line breaks, it has two concentric Token Rings [1], which increase the reliability of the backbone. The maximum circumference of the ring is 100 km (62 miles), with a maximum 2 km between stations (FDDI nodes are also known as stations). It is, thus, an excellent mechanism for connecting networks across a city or over a campus. Up to 500 stations can connect to each ring with a maximum of 1000 stations for the complete network. Each station connected to the FDDI highway can be a normal station or a bridge to a conventional local area network, such as Ethernet or Token Ring. FDDI networks can use two types of fiber-optic cable, either single-mode or multimode. The fibers most commonly used in FDDI are 62.5/125, and this type of cable is defined in the ANSI X3T9.5 standard.

Two rings in FDDI are useful for fault conditions but are also used for separate data streams. This effectively doubles the data-carrying capacity of FDDI (to 200 Mbps). However, if the normal traffic is more than the stated carrying capacity, or if one ring fails, then its performance degrades. When a station on a ring malfunctions or there is a break in one of the rings, the rest of the stations can still use the other operational ring. When a station on the network malfunctions, both of the rings may become inoperative. FDDI allows other stations on the network to detect this and to implement a single rotating ring [1]. This fault tolerance method also makes it easier to insert and delete stations from the ring. FDDI-II is an upward-compatible extension to FDDI that adds the ability to support circuit switched traffic in addition to the data frames supported by the original FDDI. With FDDI-II, it is possible to set up and maintain a constant data rate connection between two stations.

3.3.2 ATM

Asynchronous Transfer Mode (ATM) [1] is another popular technology for backbone networking using optical fibers. Many campus-wide backbones have been deployed with ATM switches connected by optical fibers. They will automatically come under the purview of PervNet. It is true that ATM technology is recently facing a serious challenge from gigabit Ethernet and WDM technologies; but there is already a good amount of investment done on it (particularly in Europe). The major objective of ATM is to integrate real-time data (such as voice and video) and non-real-time data (such as computer data). This is one of the primary requirements of PervComp too. Computer-generated data can typically be transferred in non-real-time, but it is important that the connection is free of errors. In PervComp applications, single bit error can cause serious mistake in perception or context awareness. Sensor data require a constant sampling rate and low propagation delays, but are more tolerant to errors and any losses of small parts of the data.

An ATM network relies on user-supplied information to profile traffic flows so that a connection has the desired service quality (i.e., QoS), which will be very useful in PervNet context. Computer data will typically be sent in bursts. Sometimes a high transfer rate is required (perhaps when running a computer package remotely over a network) or a relatively slow transfer (such as when reading text information).

3.3.3 Gigabit Ethernet

Gigabit Ethernet [1] was originally designed for optical fibres. Initially operating over optical fiber, Gigabit Ethernet is later extended for Category

5 UTP cabling to support compatibility. The 802.3z Gigabit Ethernet task force identified three specific objectives for link distances: a multimode fiber-optic link with a maximum length of 550 meters; a single-mode fiber-optic link with a maximum length of 3 kilometers (later extended to 5 kilometers); and a copper based link with a maximum length of at least 25 meters (discussed in the previous section). For the 62.5 micron diameter 160 MHz*km multimode (MM) fiber often called FDDI-grade fiber, the distance is specified at 220 meters. As the bandwidth of the fiber increases, the minimum range for MM fiber increases up to 550 meters. The longwave length transceiver (1000BASE-LX) reaches 550 meters for all media types. For single mode fiber with 1000BASE-LX, the distance is specified at 5 km.

Gigabit Ethernet on fiber supports new full-duplex operating modes for switch-to-switch and switch-to-end-station connections, and half-duplex operating modes for shared connections using repeaters and the CSMA/CD access method. An FDDI campus or building backbone can be upgraded by replacing the FDDI concentrator or hub or Ethernet-to-FDDI router with a Gigabit Ethernet switch or repeater. As an intermediate step, some users might migrate to an FDDI switch before installing a Gigabit Ethernet switch. The only upgrade required is the installation of new Gigabit Ethernet interfaces in the routers, switches or repeaters. All the investment in fiber-optic cabling is retained, and the aggregate bandwidth is increased at least tenfold for each segment.

3.3.4 SONET/SDH

Over the years, in the early generations of backbone optical networking, established carriers have built their optical networks with Synchronous Optical Network/Synchronous Digital Hierarchy (SONET/SDH) [1]-[5] ring architectures in North America and other locations around the world. In many ways, SONET has earned its stripes. The SONET ring architecture is a proven technology; tens of billions of dollars worth of equipment to support SONET rings has been invested by AT&T and others; and besides offering effective performance, rings also have demonstrated advantages in operating through faults in the network, and restoration of disabled rings also is fairly rapid.

But as we enter the PervNet era, there is a doubt in the mind of carriers and manufacturers [4],[5]: Will SONET rings deployed now be a noose around a carrier's ability to succeed in future? Are SONET rings enough for coping up with the bandwidth tide? The reason behind this suspicion is that SONET ring based networks do have some serious limitations, such as, inflexible architecture, poor utilization, unnecessary backup, slow provisioning, poor restoration, and high operational cost, as discussed below.

Rings can be an inflexible architecture. The typical SONET OC-192 BLSR ring, for instance, is unable to transport OC-192 Internet backbone trunks. While an increasing number of router vendors are offering OC-192 interfaces, carriers are unable to place the OC-192 circuits on their existing ADM based rings. Thus, the highest available bandwidth is never made available to the client layer elements, and the carriers have to wait for the next generation technology (viz., WDM [3]) to be available to support BLSR rings. This can create problems as networks migrate to PervNet architectures to meet the exploding demand in PervComp traffic. Additionally, for fully protected traffic, rings are unable to achieve 50 percent capacity utilization. Capacity may be available only in certain portions of a ring, but not over the entire ring, thus forcing the carrier to provision an entirely new wavelength, while unable to exploit the unused portions of the ring. Thus, full capacity cannot be utilized to carry traffic. However, carriers are still forced to dedicate protection bandwidth for non-traffic bearing capacity as well.

Another big issue is unnecessary backup. For instance, to increase capacity, carriers typically implemented SONET/SDH multiplexing with its ring architecture. Rings provide fast robust protection against multiple types of failures including the dreaded fiber cut. However, this protection comes at a severe cost– a completely redundant or duplicate network is maintained in the unlikely event of service interruption. Sitting idle, this duplicate capacity cannot be utilized to generate any revenue with current SONET/SDH equipment. Together with it, very slow provisioning has already made it a poor candidate for PervNet backbone. In a ring-based network, a typical long haul circuit has to be interconnected through many rings using expensive and inefficient back-to-back tributaries. This requires the availability of bandwidth simultaneously on all rings in order to provision the long haul circuit. In reality, however, the bandwidth may not be available in all rings, and the carrier has to wait till the next build-out for the circuit to be provisioned. In the meantime, the available bandwidth is reserved on the other rings. The end result is a very slow provisioning process. It can take many months to provision/add a new customer or augment a customer's existing service. This was acceptable when traffic growth was doubling every 20 years; PervNet obviously require a better solution. Carriers are forced to waste working capacity on their rings, and are unable to respond quickly to rapid shifts in demand. Clearly, this is not the "*bandwidth-on-demand*" capability that newer PervComp applications require. Consequently some carriers are being forced to look for other topologies.

BLSR ring protocol was specified with an additional capability, extra traffic that was meant to improve the bandwidth utilization of rings. Extra traffic was specified to use the dedicated protection bandwidth available in the ring, and was preempted in the event of a failure anywhere on the ring.

However, with no network database capability to support provisioning for end-to-end extra traffic circuits, preemptable traffic service is a no-show in ring networks. With rapidly falling prices for bandwidth, ring-based architectures are fast reaching a point where the cost of building a network exceeds the revenue they generate. Thus, SONET ring architectures are actually suitable for the legacy networks where most of the bandwidth was dedicated to voice. But, they are unable to match the requirement of dynamic flexible, just-in-time bandwidth in PervNet.

3.3.5 WDM

So far, to accommodate traffic growth, carriers have traditionally responded by adding cable and equipment and increasing traffic rates. However, in PervNet, we have to find new faster methods for increasing bandwidth, particularly at the core. Carriers could not place enough fibers fast enough to keep up with capacity demand. Wavelength Division Multiplexing (WDM) [2]-[5], due to its efficient use of bandwidth, has the potential to solve this dilemma by allowing multiple signals to use the same fiber. Recently, availability of wide-band erbium-doped optical amplifiers has opened up a new avenue for multiplexing many wavelengths into the same fiber. This multiplexing of wavelengths is known as WDM. Normally, in a WDM configuration, multiple numbers of lasers, emitting different wavelengths, are coupled together into a high-bandwidth fiber. At the receiver end, narrow-band optical filters are used to extract the desired wavelengths for respective receivers, thereby establishing several independent source-destination connections. In WDM transmission, each data channel is modulated onto an optical carrier with a unique wavelength (or optical frequency). The optical carriers are then combined and transmitted on a single fiber. In this way, WDM not only enables the use of the enormous fiber bandwidth, but also provides channels whose individual bandwidths are within the capacity of conventional electronic information-processing devices. Thus, WDM has emerged as the most promising transmission technology for optical networks in the backbone of PervNet.

3.3.5.1 Introduction

WDM optical mesh networks are fast becoming a key enabler of the new-world bandwidth paradigm [5]. The technique of WDM is to divide the huge bandwidth of an optical fiber into a number of parallel wavelength channels, where each channel can carry of data at the rate of Terrabits per second. There add-drop-multiplexing (ADM) [2] allows a part of the information carried in a transmission system to be demultiplexed (dropped) at an intermediate point and different information to be multiplexed (added) for subsequent transmission. The remaining traffic passes straight through the multiplexer without additional processing. Thus, ADM is capable of extracting and inserting lower-rate signals from a higher-rate, multiplexed signal, without completely demultiplexing the signal. WDM promises advantages for switching and routing as well as for transmission. Optical cross-connects (OXCs) [3]-[5] are currently being developed which can switch an entire wavelength from an input fiber to an output fiber so that large bandwidth circuits can be routed through the network according to wavelength. High-speed, fixed-bandwidth, end-to-end connections, called lightpaths [5]-[7], can then be established between different nodes. Networks which use OXCs to route lightpaths through the network are referred to as wavelength-routing networks [2]-[7]. Wavelength-routing optical core networks are expected to evolve from the existing separate WDM transmission systems to form optical layers in future transport networks. Recent advances in optical technology have resulted in an exponential increase in traffic-carrying capacity of optical equipment. From only a few tens of wavelengths in 1996, WDM technology has progressed so rapidly that equipment are capable of supporting several hundreds of wavelengths per fibre. With today's Dense WDM (DWDM) [5], the capacity of a single fiber has increased more than 200-fold.

But, higher rate optical channels, such as OC-192s, need: a) multiple frequencies, not time slots, b) hundreds, not tens, of wavelengths, c) switch integrated ADM functionality, not individual ADMs, and d) mesh networks tailored to datagram flows, not point-to-point connections designed for predictable voice traffic. Implementing such techniques by overlaying stacked SONET rings with point-to-point WDM creates a *non-scalable* architecture. As a result, many carriers are now finding a solution in optical mesh design. Subsequently, the market for OXCs, on which mesh networks are built, is slated to jump to $1.8 billion by 2003. Moreover, with optical mesh, a carrier is not restricted to purchasing a stack of equipment for enabling an extra wavelength on the stacked ring. So WDM will play a major role in developing the PervNet infrastructure, and in bringing on the solutions that will take us to the next generation PervNet environment. Accordingly, carriers are now forced to take stock of their network architectures, and decide whether or not the path to the future follows the traditional *ring* architecture or the optical *mesh* topology [5]. Choices made now will have a major impact on how PervNet will perform in the years to come. DWDM mesh networks, however, does not hold all the answers to solving bandwidth demand. We need intelligent switching too (discussed afterwards).

3.3.5.2 Network Architecture

A typical WDM mesh network is a set of optical wavelength routers (i.e., OXCs) interconnected by pairs of point-to-point fiber links. For example, the network of Figure 3.2 consists of: a) an all-optical inner portion which contains the wavelength routing cross-connection (or switching) elements, each capable of independently routing an incident wavelength, and b) an outer portion which contains user access stations which attach to the optical medium. The WDM core permits a limited number of wavelengths available to each link to enable full virtual connectivity, if desired, among all users. The wavelength routers have the ability to route an incoming signal to an outgoing port according to the signal's input port and wavelength. Wavelength-routing networks employ "spatial reuse" of wavelengths, by allowing the same wavelength to be used by multiple lightpaths in the same network, providing that none of these lightpaths share a common link. This allows scalability of wavelength-routing networks, although this scalability may be limited in non-reconfigurable networks [3]-[7].

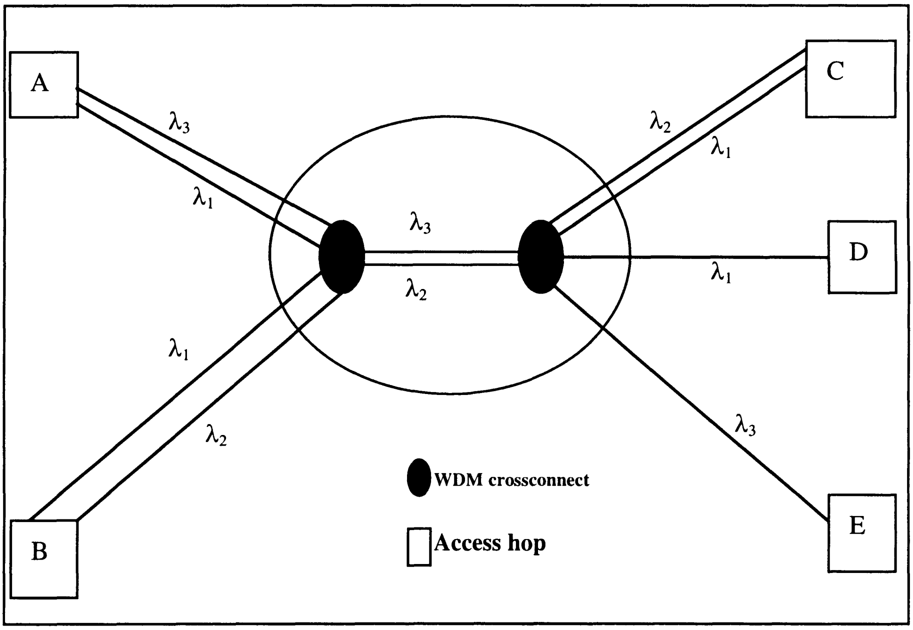


Figure 3.2 WDM optical network

In Figure 3.2, WDM cross connects are shown within the circle constituting the optical portion, and the squares represent the network access stations. An OXC acts as a wavelength router that receives a message at some wavelength from an input fiber and redirects it to any one of the output fibers at the same or different (if wavelength conversion facility is available at that router) wavelength. Wavelength λ_3 carries a one-optical-hop signal (no intermediate detection or *wavelength translation*) from node A to node E, while a signal from node A to node C is carried in two optical hops: A to B on λ_1 and B to C on λ_2. Wavelength λ_1 is reused to carry a signal from C to D. Since the number of receivers and transmitters per access station is limited, the optical connectivity among the stations is not full. Thus, most of the end-to-end connections will require multiple hops, through a sequence of optical channels or lightpaths. These connections are referred to *virtual connections* [6],[7]. The full virtual connectivity is possible by using intermediate stations cooperating as relay nodes. When a new virtual connection request is generated, the job of the admission controller is to decide whether to admit or block the request by finding a path capable of handling the virtual connection. A virtual connection request is blocked, if the controller is unable to find or create a path, without unacceptably degrading the quality of service enjoyed by other virtual connections. These virtual connections define a *virtual topology* [6], consisting of lightpaths as links and routing centres as nodes, on a given *physical topology* of WDM optical network. We shall discuss about them shortly.

3.3.5.3 Advantages of Mesh Networks

While optical ring networks are well understood by the current literati, much less is broadly known about mesh networks. In mesh topologies, theoretically, each point in a network has a pathway to every other point in the network. Mesh networks, built on OXCs, exploit a combination of IP and SONET based mechanisms to provide dynamic provisioning and fast deterministic shared protection. The benefits of mesh topologies for optical networks are:

- **Scalability:** Mesh topologies provide services at the highest line rate, and can work seamlessly with IP routers. They enable routers to dynamically request and release bandwidth for relief on congested routes.
- **Just-in-time Bandwidth:** Utilizing dynamic mechanisms that are inherent in the IP protocol, mesh architecture enables point and click bandwidth solutions. This capability becomes increasingly important in PervNet for two reasons: 1) as bandwidth prices decline rapidly, carriers need other means to differentiate themselves; and 2) with unpredictable demand patterns that are getting tougher to forecast, carriers need to be able to configure bandwidth on demand in order to prevent severe congestion in parts of their network.

- **Better Utilization:** Mesh architectures can offer utilization rates of 70 percent or more. Mesh also provides intelligent and flexible protection sharing.
- **Dynamic Provisioning:** With end-to-end dynamic provisioning support, mesh networks on the other hand provide a unique capability to exploit preemptable traffic. For instance, a router requesting temporary bandwidth for congestion relief may provision a preemptable circuit on demand. The short duration preemptable traffic is able to utilize the idle protection capacity without any significant impact on reliability. The likelihood of preemption is extremely low.
- **Network Restoration:** The mesh architecture also supports Quality of Service (QoS) features that make more sense for the mixed voice, data and Internet traffic that characterizes PervNet needs. Circuits can be provisioned while taking into account restoration priorities, and restoration times. This flexibility avoids the one-size-fits-all approach taken by ring-based networks. Mesh also allows the carrier to provide restoration times comparable to those of stacked rings for voice traffic.
- **Operating Costs:** Operational savings through optical mesh topology can be as high as 60 percent compared to ring structures. A ring network, with its dedicated backup bandwidth, uses between two and four times the number of line cards of a mesh network of similar capacity (depending on the degree of connectivity of the nodes, and the demand patterns).

3.3.5.4 Lightpath Establishment

Despite its similarity with the routing problem in conventional circuit switched network, routing in optical mesh networks is unique. There are two ways by which data can be sent from a source node to a destination node, which is more than one hop distant, in a WDM wavelength routed network [3]-[7]. Firstly, we can use different wavelengths in different hops. Secondly, we can first find out if a wavelength is available throughout the path and then use it. The former is obviously better in reducing the blocking probability. But the study of opto-electronic wavelength converters has shown that delay in former case is so large that it will fail to meet the requirements of PervNet. In the latter case, prior to be admitted, each call requires a wavelength connection to be established from source to destination. This eliminates the needs for buffering and opto-electronic conversion at intermediate nodes. A message is transmitted from one routing node to another routing node through a wavelength continuous path by configuring the intermediate routing nodes on that path. Such a wavelength continuous path is known as a *lightpath* [3]-[7]. So a lightpath consists of a path between source-destination (s-d) pairs (or, end nodes) and a wavelength on that path. For example, in Figure 3.3, there are 8 lightpaths shown in different colours. If only lightpaths are allowed in a network, then there are no optical-to-electronic conversions, and thus no question of electronic delay at intermediate nodes along the lightpath. But, two lightpaths that share a common link in the network must use different wavelengths. In other words, the same wavelength must be used on all the links along the selected path. This is known as the *wavelength continuity* constraint [7]-[11]. Due to this constraint, which is unique to WDM networks, wavelength channels may not always be utilized efficiently.

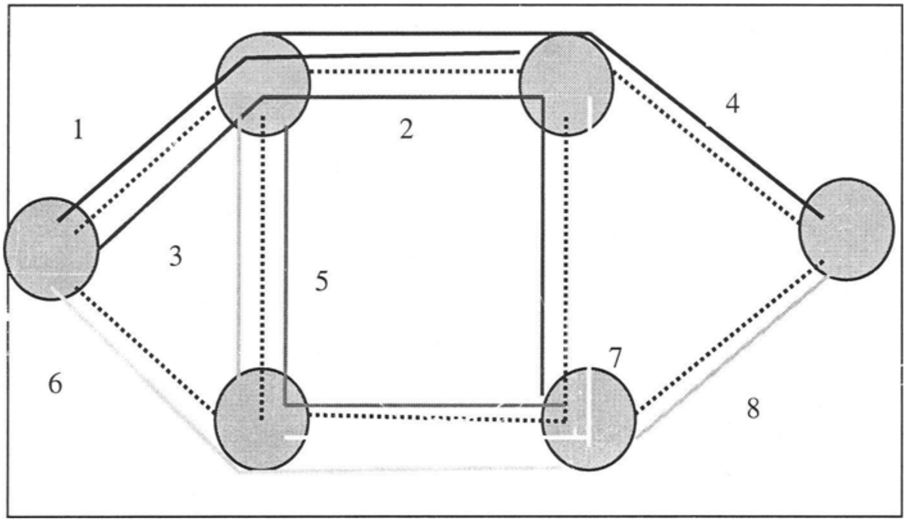


Figure 3.3 Lightpaths in a WDM network

Obviously, in a network with N nodes, the ideal situation would be to have the capability of setting up lightpaths between all N*(N-1) node pairs simultaneously at any moment. But, as discussed above, this is usually not possible because of the wavelength constraint. So a connection request may be blocked, if no wavelength is available on a suitable path between the corresponding s-d pair. Consequently, the blocking probability increases significantly for lightpaths requiring many consecutive links. A possible alternative could be to re-shuffle the assignment of existing calls, when a new call tends to be blocked, so as to free a wavelength for the arrived call. However, for an unrestricted topology, this method compensates only partially for the wavelength limitation at the cost of increased complexity in network operation and management [3]-[8].

So an immediate solution to this problem is the use of *wavelength converters* at some intermediate nodes, turning the network into a circuit switched network. Although the converters add substantially to the cost of the network, this is at present seems to be the potential alternative to tackle the problem. For the class of optical networks with conversion facility, there is the notion of *semilightpath* which is a transmission path obtained by establishing and chaining together several lightpaths. In a semilightpath, wavelength conversion is required at some intermediate nodes, but generally not at all nodes. Therefore, in a WDM mesh network, the route may be either a *lightpath* (i.e., wavelength continuous channel) or a *semi-lightpath* (i.e., wavelength-converted channel) [6]. A large number of procedures using the concept of shortest-path (SP) (viz., Dijkstra's algorithm), either directly or indirectly, have been suggested in the literature for computing optimal routes in the case of lightpaths [7]-[9] as well as semilightpaths (viz. Shortest path algorithm for wavelength graph [6]).

Usually, a lightpath LP_i is uniquely identified by a tuple $<\lambda_i, P_i>$, where λ_i is the wavelength used in the lightpath and P_i represents the physical path (i.e., concatenation of links) corresponding to LP_i. Two lightpaths LP_1 $<\lambda_1, P_1>$ and LP_2 $<\lambda_2, P_2>$ can share the same fiber, if and only if they use different wavelengths i.e., $\lambda_1 \neq \lambda_2$. The problem of establishing lightpaths, with the objective of minimization of the required number of wavelengths or minimization of the lightpath blocking probability, for a fixed number of wavelengths, is termed as the *lightpath establishment problem* (LEP) [7]. Usually, lightpath establishment is of two types. One is *static* (SLEP) or proactive [7], where a set of lightpaths and their wavelengths are identified a priori. Another is *dynamic* (DLEP) [11], where lightpath management is on-demand, i.e., they are established and terminated on the fly. A good survey of the existing formulations for LEP can be found in [6] and [7]. A number of heuristic algorithms for assigning wavelengths in WDM optical networks are available in the literature [2]-[7]. An overall review of these algorithms is also available in [7]. The static lightpath establishment problem (SLEP) can be formulated as a mixed-integer linear program, which is NP complete [2]. In order to make the problem more tractable, SLEP is normally partitioned into *two* sub-problems: *routing*, and *wavelength assignment.* Each sub-problem can be solved separately. On the other hand, the dynamic (on-line) version [11] considers random connection arrival times and departure times and assigns wavelengths on a per-connection basis.

3.3.5.5 Virtual Topology Design

The complete design of an optical WDM mesh network usually consists of the following four steps: 1) determination of a feasible virtual topology consisting of lightpaths as links and routing centres as nodes, 2) routing the lightpaths over the physical topology, 3) assigning wavelengths optimally to various lightpaths, and 4) routing traffic on the virtual topology. This design problem is often referred to as "*optimal virtual topology design problem*" in the literature. It has been studied extensively in [2]-[7],[13] and has been conjectured to be NP-hard [2], which means that it cannot be solved optimally for large problem sizes, unless some form of heuristic search method (such as genetic algorithm [13], simulated annealing [2], so on) is used. Most of the proposed methodologies [6] have suggested of using a regular topology, such as hypercube, as a virtual topology. Regular topologies, no doubt, offer several advantages, such as 1) simplified routing and congestion control procedures to reduce the amount of electronic processing required at each node, and 2) simplified network implementation due to standard hardware requirements at each intermediate node. But, on the negative side, in regular topologies, asymmetric traffic patterns create bottlenecks, thereby substantially deteriorating the overall system performance (i.e., increasing average delay and average hop length). To alleviate this problem, topology embedding must take into account traffic patterns in the system [12]. Some have studied the mapping of regular structures into a WDM star, considering the traffic pattern imposed on the system, so that mapping will optimise system throughput. Some have studied the embedding of unidirectional incomplete hypercube into the physical topology. Some uses the physical topology as a subset of the virtual topology, employing algorithms for maximizing the throughput, subject to bounded delay characteristics.

But it is always better to study a general version of the problem [13] so that arbitrary virtual topologies can be embedded on a physical fiber network. In particular, WANs, such as NSFNET's T1 backbone network (Figure 3.1), are to be considered so that the design can be targeted for nation-wide coverage. Assume that the following inputs are given: 1) a physical fiber topology, where each node is equipped with wavelength routing switches (WRS), 2) number of wavelength channels carried by each fiber, 3) a traffic matrix, and 4) number of transmitters and receivers available at each node. The outputs that are to be produced are: 1) a virtual topology of lightpaths, 2) wavelength assignment for the links of the virtual topology, and 3) sizes and configurations of wavelength routing switches at intermediate nodes. Two independent objectives (optimality criteria), useful for PervNet, may be: 1) maximize throughput, and 2) minimize network-wide average packet delay, for a given traffic matrix. The first objective is mainly concentrated on throughput and is expressed in terms of scale factor (scale-up) i.e., by what factor elements of a given traffic matrix can be multiplied so that the network can still carry the scaled up traffic. This obviously attempts to address the scalability issue of PervNet. The mathematical formulation of this problem is given in [2] and [13], where an integer scale factor is considered.

Consider any arbitrary virtual topology, which can be regular or irregular, for embedding into a physical topology. So, the problem of asymmetric traffic flow present in a regular topology is overcome. While optimising throughput, the simplified routing offered by regular topology is traded off, as it is not so important in this case. Consider a fixed number of wavelength channels permitted per fiber and generate virtual topologies randomly. First a tree based on a random Prufer number [13] is generated. Next, add and/or delete edges from the tree until the randomly generated connected graph satisfies transmitter and receiver constraints at all nodes. For embedding a virtual topology into a physical fiber network, a heuristic algorithm is developed in [13], which considers the number of wavelengths per fiber as fixed. For assigning wavelengths [12] optimally to various lightpaths, while not violating physical constraints, a heuristic algorithm is used, where wavelengths are assigned to lightpaths in the decreasing order of number of disjoint lightpaths (i.e., lightpaths that do not share the same physical link). For routing of packets in virtual topology, the well-known flow deviation algorithm is used. This algorithm is based on the notion of shortest path flows. It first calculates the linear rate of increase in delay with an infinitesimal increase in the flow on any particular channel and then uses these lengths for shortest path routing. For optimization, genetic algorithm is used. First, a number of random feasible virtual topologies, to be used as the initial population in the genetic method, are generated. Then, these virtual topologies are encoded as strings, and suitable fitness functions are chosen for the afore-mentioned optimality criteria 1) and 2) separately. Next, selection, crossover and mutation operations are repeatedly performed on the initial population, after choosing suitable control parameters such as mutation rate, crossover rate and population size. These operations are repeated until termination criterion is reached. The solution obtained at this point is taken as the optimal solution.

3.3.5.5.1 Generation of Arbitrary Virtual Topology

The virtual topologies are generated randomly, where each topology must satisfy three constraints: i) It must be connected i.e., there must exist at least one path between every pair of nodes, ii) The outdegree of every node must be less than or equal to number of transmitters available at each node, and iii) The indegree of every node must be less than or equal to number of receivers available at each node. An effective strategy is required to generate random topologies that satisfy all the above constraints. Otherwise, it will be very much time consuming for generating even a single topology that satisfies all three constraints. Since a connected topology is required, start with a tree, which is a connected graph. For this, assume that outdegree (indegree) of each node in virtual topology is equal to the maximum number of transmitters (receivers) available at that node. This additional assumption not only simplifies the problem, but also helps find a good solution (because throughput is maximum when we consider maximum degree of nodes).

Prufer number [13] can be associated with a tree in the following manner. Let T be a tree of N nodes. The Prufer number, P(T), is an (N-2) "digit" number where digits are numbers between 1 and N and are defined by the following algorithm:

1) Let i be the lowest numbered leaf (node of degree 1) in T. Let j be the node, which is predecessor of i. Then, j becomes the rightmost digit of P(T). We build P(T) by appending digits to the right. Thus, P(T) is built and read from left to right.
2) Remove i and the edge (i,j) from further consideration. Thus, i is no longer considered at all, and, if i was the only successor of j, then j has become a leaf.
3) If only two nodes remain to be considered, Stop because P(T) has been formed. If more than two nodes remain, return to step 1.

Conversely, generate a tree from a Prufer number via the following algorithm:

1) Let P(T) be the original Prufer number, and let all nodes, not part of P(T), be designated as eligible for consideration.
2) If no digits remain in P(T), then there are exactly two nodes, i and j, still eligible for consideration [as we remove a digit from P(T) in step 3 below, we remove exactly one node from consideration, and there are N-2 digits in the original P(T)]. Add (i,j) to T and Stop.
3) Let i be the lowest numbered eligible node. Let j be the leftmost digit of P(T). Add the edge (i,j) to T. Remove the leftmost digit from P(T). Designate i as no longer eligible. If j does not occur anywhere in what remains of P(T), designate j as eligible.
4) Return to step 2.

So, first generate a Prufer number randomly. Any "digit" in the Prufer Number is repeated at most one less than the number of transmitters available at the node corresponding to the "digit". Then, an undirected tree is constructed from the Prufer number by the algorithm given above.

The tree can be represented in adjacency matrix form. The 1's in adjacency matrix are made permanent. New edges are then added to the already constructed graph so that number of 1's in any row of adjacency matrix equals the number of transmitters available at that node corresponding to the row. The resultant topology obtained is a connected topology that satisfies transmitter constraint at every node. Next, in order to verify the receiver constraint for each node i, we calculate EXCESS(i), where EXCESS(i) is defined as follows: EXCESS(i) = Indegree of node i - Number of receivers available at node i. Indegree of node i is calculated by counting the number of 1's available at i-th column of adjacency matrix. Clearly, EXCESS(i)>0 means that node i has an indegree greater than the number of receivers available at that node. EXCESS(i)=0 means that indegree of node i equals the number of receivers available at node i, while EXCESS(i)< 0 means that indegree of node i is less than the number of receivers available at node i. So, for each node i having EXCESS(i)=0, mark the 1's and 0's at i-th column permanent. Next, in each pass, the nonpermanent node i having maximum positive EXCESS value and the node j having maximum negative EXCESS value are identified. Then, in the adjacency matrix, 1' s that are in column i are exchanged arbitrarily with as many 0's that are not permanent in column j, keeping row fixed. This can be done at most *min*(absolute(EXCESS(i)),absolute(EXCESS(j))) times. After the operations are performed, 0's and 1's that are exchanged are made permanent. If no exchange operation can be performed, node j is marked temporarily deleted, and, from the rest nodes, another node having maximum negative value is considered. If all nodes having negative EXCESS values are temporarily deleted, then the current topology cannot be used further. Otherwise (i.e., if, at least, one exchange operation can be performed), all temporarily deleted nodes are undeleted. If, after exchange operation, EXCESS(i) becomes zero, then node i is permanently deleted. Also, if EXCESS(j) becomes zero, then node j is permanently deleted. After EXCESS(i) becomes zero, another node, that has positive EXCESS value and that is not permanently deleted, is chosen as i. If all nodes (including permanently deleted, temporarily deleted and undeleted) have EXCESS value either zero or negative, then the topology thus generated satisfies the receiver constraint. If the topology does not satisfy receiver constraint, then another random topology is generated and the above operations are repeated.

3.3.5.5.2 Embedding of Virtual Topology

Embedding means mapping of virtual topology to physical topology without violating the constraints. Node exchange operations for embedding arbitrary virtual topology to physical topology are studied in [2], [6]. An approach [13] that does not take into account number of wavelength channels permitted on a physical fiber as a constraint is described here. This algorithm uses one heuristic evaluation function. For each successive pass of the algorithm, one link from virtual topology is taken, and an attempt is made to find the best path having minimum cost based on the heuristic evaluation function. The complete algorithm is given below:

1) For each physical link i,

- calculate COST(i), where COST(i) = Normalized_length(i). The normalized length of a link is calculated by dividing the length of the link by the length of the longest link.
- set NO_OF_VLINK_ASSIGNED(i) = 0, where NO_OF_VLINK_ASSIGNED(i) indicates, at any point of the algorithm, how many virtual links have thus far used the link i for embedding.

2) Amongst the virtual links (x,y) that are not yet embedded, find the one which, if embedded along shortest path between node x and node y in physical topology based on cost of all links that are not yet deleted, will take minimum number of physical links. In case of a tie, take that virtual link which will take less cost in embedding in shortest path. Let this virtual link be (u,w). If embedding is not possible for all virtual links that are not yet embedded, then return FAILURE. Otherwise, virtual link (u,w) is embedded to the shortest path found in physical network. Also, NO_OF_VLINK_ASSIGNED is incremented by 1 for each link in physical topology that lies in the shortest path.
3) If, for any physical link i, NO_OF_VLINK_ASSIGNED(i) equals the number of wavelength channels permitted per physical fiber, then the link i is considered deleted (i.e., not considered for next passes).
4) Revise COST of each physical link i that is not deleted as follows: COST(i)=W1*NO_OF_VLINK_ASSIGNED(i)+W2*Normalized_Length(i), where W1 and W2 are two weights.
5) If no more virtual links remain for embedding, then return SUCCESS. Otherwise, go to step 2.

The performance of this heuristic algorithm depends on a suitable choice of weights W1 and W2. The rationale behind the cost revision operation is that, as a virtual link uses a particular physical link for embedding, it becomes costlier so that unassigned virtual links try to avoid that particular physical link so long as a better path is found. The normalized length is used in evaluation function so as to take into account for propagation delay which increases with increase in length of link. The variable NO_OF_VLINK_ASSIGNED indicates feasible part of embedding solution. The shortest path is calculated by Dikjstra's algorithm [7]. An example of the implementation of this embedding algorithm can be found in [13].

3.3.5.5.3 Wavelength Assignment

Given an embedding, all the virtual paths can be determined that pass through a physical link. Next, we need to assign wavelengths to lightpaths in such a way that any two lightpaths passing through the same physical links are assigned different wavelengths. Assigning wavelength (colors) to lightpaths, so as to minimize number of wavelengths (colors) under the wavelength continuity constraint, reduces to the well-known graph-coloring problem. This problem is NP-complete, and the minimum number of colors needed to color a graph G (called chromatic number) is difficult to determine. A mathematical formulation of the problem can be found in [12].

Assume that number of wavelengths available is not a constraint. But this approach is, as far as possible, to minimize number of wavelengths used. A heuristic algorithm for wavelength assignment is use and is, to a large extent, similar to the wavelength assignment heuristic given in [12], where one-optical-hop traffic is maximized. It is a greedy algorithm, which attempts to assign each wavelength to as many connections (i.e., lightpaths) as possible without violating the physical constraints. Here, use the same wavelength channel for two or more different conversations at the same time, without violating any physical constraint, known as wavelength reusing. The algorithm first generates connection link indication matrix [12]. In this matrix, each connection corresponds to one column (or row). In this algorithm, "connection" and "column" are used interchangeably. The algorithm is given below:

1) Generate the connection link indication matrix M = ($m_{(ij),(lm)}$), where $m_{(ij),(lm)}$ = 1, if virtual links ij and lm uses a common link, and 0 otherwise. Then, order the rows and columns in the non-decreasing number of 1's in it.
2) Initialize W=1, where W indicates the wavelength number.
3) Repeat steps (4) through (8) until all links in the virtual network are assigned unique wavelength numbers. At last, go to step 9.
4) Assign the wavelength W to connection (row or column) i having smallest number of 1's.
5) Remove temporarily connection j (i.e. row and column j) with $m_{k,j}$ =1 for j=k+1, k+2, ..., N.
6) Assign the wavelength number W to the connection not removed from the matrix which is having the least number of 1's, say connection s, where s>k. If s exists, set k=s and go to step 5.
7) Otherwise (i.e., no such s exists), undelete the rows and columns (i.e., connection) that were temporarily deleted from M, and remove the rows and columns corresponding to the connection which has been assigned wavelength number W.
8) Set W= W+1.
9) Set P=W-1, return P where P is the number of wavelengths used.

The above algorithm is tested and used for generating solutions in this work reported in [13].

3.3.5.5.4 Traffic Assignment

Flow deviation method has already been used for the traffic assignment problem for minimizing network-wide average packet delay. The same flow deviation algorithm for traffic assignment in a virtual topology may also be used. The flow deviation algorithm requires one feasible starting flow, which can be iteratively improved. In [13], starting solution is found by just finding shortest-path routing. Another algorithm for initial assignment is proposed where first sort the node-pairs in the traffic matrix in descending order of traffic. Then, take the node-pairs (i.e., source node and destination node) in the sorted order one by one and assign the traffic in the shortest path based on minimum number of links. If full amount of traffic cannot be assigned in the shortest path, then the maximum possible amount is assigned, and those links that are fully saturated are marked deleted. The rest amount is repetitively assigned in shortest path using the remaining links. Clearly, this approach will tend to optimize throughput as it assigns greater amount of traffic with lesser number of links. For maximum scaleup, the theoretical limit of maximum scaleup by dividing total capacity of the virtual network by total amount of external traffic is calculated. Next, any convenient search technique (such as binary search technique) can be used to find maximum scaleup in the range 1 to theoretical limit of maximum scaleup.

3.3.5.6 Routing and Wavelength Assignment (RWA)

RAW is one of the most widely analysed and conversed problems in designing next generation WDM networks as several researchers [7] have studied the problem of routing in WDM networks as an optimisation problem to be solved by efficient heuristics. Among the various formulations, Ordered Shortest-Path Algorithm by Ramaswami and Sivarajan [3], Simulated Annealing by Mukherjee et. al. [2], Iterative Approach by Zhang and Acampora [12], Layered Graph Approach by Banerjee and Chen [7], Rounding Approach by Banerjee and Mukherjee [2]. MILP (Mixed Integer Linear Programming), HLDA (Heuristic Logical Design Algorithm), MLDA (Minimum-delay LDA), TILDA (Traffic Independent LDA), and RLDA (Random LDA) proposed by Ramaswami and Sivarajan [3], lightpath-based one-hop Traffic Maximization scheme of Banerjee, Yoo, and Chen [7], and Genetic Algorithmic approach of Saha et. al. [13] are worth mentioning. The essence of this line of approach is first generating an auxiliary graph (or matrix) indicating the link sharing, and, then based of that graph, assigning wavelengths to the lightpaths following the wavelength continuity constraints.

In Banerjee and Mukherjee [2], the optimized logical problem is broken into a number of smaller sub-problems allowing each one to be solved independently and efficiently. Three sub-problems are identified and the results from one sub-problem are fed to the next one. Sequential *graph coloring algorithms* are used to assign wavelengths to the lightpaths by taking into account the wavelength-continuity constraints. Both SLEP and DLEP are studied. First the paths are determined, and, once the paths have been calculated, each path is then represented as a node of the path graph. WAP posed as the graph coloring problem. The sequential graph coloring approach is illustrated, where vertices are sequentially added to the portion of the graph already colored.

Ramaswami and Sivarajan [3] have proposed a formulation of the optimal RAW problem for the deterministic case. The objective function maximizes carried traffic. Formulation is given for traditional circuit switched as well as optical circuit switched network. It is shown that, by dropping integrality constraints, the upper bounds on maximum carried traffic in both optical and traditional circuit switched networks are the same. A better formulation based on *path graph* is also proposed. In path graph G_p, each node corresponds to a path in $G_{physical}$. Two nodes in G_p are connected if and only if the corresponding two paths in $G_{physical}$ share a link. Then, the RAW problem becomes equivalent to the *path graph-coloring* problem. It is shown that the solutions to this formulation are asymptotically optimal for large number of wavelengths, assuming that calls arrive at random and have random holding times.

Zhang and Acampora [12] has proposed three formulation of RWA problem which are: (1) CP: a non-linear integer program, (2) CP_{mix}: a mixed linear program, and (3) CP_1: CP with one wavelength. The non-linear integer program (CP) is difficult to solve when N and W are large. By introducing additional continuous variables, the non-linear integer program CP is converted to a mixed integer linear program CP_{mix}. The problems CP and CP_{mix} can be further decomposed into W iterative binary linear integer sub-problems. This is equivalent to solving the WAP W times. Though the size of CP_1 is considerably smaller than those of CP and CP_{mix}, it can still be impractical to solve for larger number of nodes. The complexity of the algorithm is $O(N^4)$. A connection-link indication matrix is generated first. The algorithm iteratively assigns each wavelength to as many connections as possible while satisfying physical constraints. The objective is to maximize the amount of one-hop traffic. Wavelengths are assigned to the connections in decreasing order of their traffic demands.

3.3.5.7 Wavelength Reservation

In DLEP, setting up a lightpath can be done in various ways [8]-[11], which can be broadly classified into two categories: centralised and distributed. In the centralised approach [8], there is one master router, which keeps all information about paths and wavelength usage. Whenever a node requires any information about the topology or routing, it has to consult with that master router. But, in large networks, this centralised approach is not feasible because the master node can not keep up with the updating of topology as well as the wavelength usage made by all other nodes which are supposed to be running in parallel. Moreover, if this master node crashes, all the necessary information will be lost, which is not at all tolerable in this dynamic situation. Another problem is that, when two connections are going to be set in the same link from different directions, there may exist a race condition for which both the paths will be blocked.

On the other hand, in distributed control [11], every node acts as a local controller and maintains a local table describing necessary internal data structures. Nodes can update this table without any delay. Also, if one (or more) node crashes in the network, other nodes will still continue to work properly. So this system is robust and reliable. But there is a drawback. As the nodes do not have global information about the network, collision may occur if path establishment for two contemporary connection requests is initiated on a particular link from both directions.

A distributed reservation protocol, under the condition of rapidly changing availability of resources in a WDM network, should correctly and efficiently reserve necessary and available wavelengths during lightpath (i.e., connection) set-up and again release those resources when they are no longer needed. This reservation is normally accomplished with the help of a few control packets exchanged between the source-destination pair prior to the start of data transfer. There are two classes of distributed reservation protocols [11], namely *forward reservation*, and *backward reservation.* Forward (backward) reservation protocol is also known as source (destination) -initiated protocol because the source (destination) node begins the actual reservation process. In both reservation protocols, the source node sends out the first control packet towards the destination node either to reserve (forward) or to probe (backward) the available wavelengths enrouted. The destination node selects one of the reserved (forward) or potential (backward) wavelengths and issues the second control packet back to the source node to release the unselected wavelengths (forward) or to reserve the selected wavelength (backward). These protocols are described next.

3.3.5.7.1 Forward Reservation Protocols (FRPs)

In this technique, the source node sends a reservation (RESV) packet to the destination node along the decided route, once a connection request has arrived. Each node along the path processes the RESV packet and temporarily locks one or more appropriate wavelengths on the next link for the connection. If no suitable wavelength is found on the next link, that intermediate node sends a failure (FAIL) message back to the source. FAIL packet unlocks all the wavelengths reserved so far. Otherwise, at the destination, one of the available wavelengths is picked up and a confirmation (CONF) packet is sent back from destination to source. On its way back to the source, this CONF packet permanently locks the selected wavelength and unlocks the other wavelengths at the intermediate nodes. There are many variations of FRP, which are discussed below.

Exhaustive: In this case, all available wavelengths in all hops in the selected path are reserved. This protocol is good for the call for which the lightpath is being set up, but is equally bad for the other contemporary calls which find the resources unnecessarily blocked. Several refinements can be suggested to overcome this drawback resulting into the modified protocols described next.

Selective all: In this case, all the available wavelengths in any hop are not blindly reserved like the exhaustive protocol. Only those wavelengths are reserved, which are already reserved in the previous hop, because a wavelength unavailable in any intermediate hop is surely going to be rejected at the destination.

Selective-N: This is a minor variation of the selective protocol. Here also, a wavelength at any hop will be reserved, iff it is also reserved in the previous hop. But there is an upper limit (say, N) on the number of wavelengths that can be reserved in any hop. By this technique, the probability of finding a lightpath for the call under consideration decreases, but, at the same time, the probability of finding a lightpath for its contemporary calls increases. So the overall efficiency increases [11]. It can be noted that, when N is equal to the number of wavelengths/fibre, this protocol becomes selective all.

Selective-N with intermediate unlocking: One major disadvantage of the selective protocols is that, when a wavelength, which has been reserved in the previous hops, is no more found available in the next hop, it is not immediately freed in the previous links although it can never be selected at the destination. Rather, it is released afterwards when the second control packet comes back to the source. Therefore, this particular wavelength resource remains unutilized for quite sometime. It is particularly noticeable in large networks where wavelength paths span multiple hops. In the proposed protocol, this disadvantage is removed. This protocol is termed as *selective-N with intermediate unlocking* (SNWIU) facility [9]. It's working is similar to selective-N protocol except the following modification.

Whenever a node finds that a handful number of wavelengths has already been identified as unavailable over one/more hop(s), an intermediate control packet is sent back immediately to the source from the node to release the wavelengths in the previous hops up to the source. This certainly consumes bandwidth of the control channel, but it increases the probability of other calls to find a lightpath. Thus, the overall performance of the network increases at the cost of a little control overhead. Details can be found in [11].

3.3.5.7.2 Backward Reservation Protocols

To overcome the main disadvantage of temporarily locking wavelengths (not used finally) in forward reservation, an optimistic approach called backward reservation is proposed [10]. In *backward reservation protocol* (BRP), a source node sends a probe (PROB) packet to the destination instead of a RESV packet. This PROB packet only gathers the wavelength usage information along the path and does not lock any wavelength. Upon receiving the PROB packet, the destination node decides upon the wavelength to reserve and sends back a RESV packet, which locks the wavelength (if it is still available) along the reverse path towards the source node. If the wavelength is not found available at some intermediate node, the node generates a FAIL packet to the destination and a NACK packet to the source. The FAIL packet releases the wavelength locked so far, and NACK packet informs the source about the connection failure.

The main drawback of BRP is that two contemporary connections, sharing one or more common links, can accidentally select the same wavelength, because both of them have found the wavelength available by their respective first control packets. So one of them will be blocked, though other wavelength(s) may be available for the connection. Hence, there will be an unnecessary blocking which is not logically tolerable. To avoid this problem, the following enhancement [11] of BRP is used.

Backward reservation with retries: Intuitively, if a connection is blocked accidentally, it should get another chance to start afresh with a new wavelength from the wavelength pool created at the destination. So, when the failure is reported back to the destination, it selects another wavelength from the available pool, and a retry is made to find out whether the second wavelength is available. If this attempt fails too, then another retry can be made provided a third wavelength is available. The more is the number of retries, the less is the chance of blocking and, hence, the better is the performance. But retries will obviously introduce extra delay in set-up time. Details can be found in [11].

Reservation or probing of wavelengths can be either *conservative or aggressive* [9]-[11]. Aggressiveness defines how many wavelengths are to be considered for reservation/probing to establish a connection on a selected path. This has a maximum value equal to the number of wavelengths available per link and a minimum value of unity (conservative). Here, we assume that each of the links in the network contains the same number (W) of wavelength so that aggressiveness varies from W to 1. Forward (or, backward) protocol uses a vector in RESV (or, PROB) packet to lock (or, note) the available wavelengths on the path. Size of this vector depends upon the aggressiveness considered. In both FRP and BRP, after the wavelength availability information reaches the destination, the destination selects a wavelength from the available set. This selection process may be one of the standards available in the literature [2],[3], say *random* selection.

3.3.5.8 Intelligent Optical Switching

While DWDM significantly increases the capacities of networks, there is still a need to more rapidly and cost effectively harness that raw capacity and deliver new optical services dynamically [14]. *Intelligent optical switches* are that answer. By providing cohesive unity between DWDM and SONET/SDH architectures, these switches combine hardware advances and sophisticated software intelligence to implement innovative features based on emerging routing and signalling standards. Intelligent optical switches support both ring and mesh architectures, allowing service providers to evolve their existing infrastructures while immediately cutting both capital and operating costs. Whereas ring architectures mandate the reservation of 100% excess capacity, mesh architectures leave the choice of protection to the service providers themselves, reducing costs by as much as 70% without compromising critical restoration times. Intelligent optical switches are, thus, the key components to evolve the PervNet to support dynamic provisioning, sophisticated high bandwidth applications, remote performance monitoring and a reduction of duplicate restoration capacity.

Intelligence in the core enables new automated management functions [15]. By converging the functions of digital cross connects and core add-drop multiplexers, intelligent optical switches perform the same functions as SONET/SDH but at lower capital and operating costs. And through the convergence with DWDM capacity, optical switches improve network reliability and intelligence. These new capabilities permit carriers to increase network efficiency and capabilities from a smaller footprint that utilizes less power thus allowing carriers to raise the bar on profitability. And, using mesh architectures, service providers can offer their customers the level of protection they desire, from none through dedicated mesh protection.

3.3.5.9 All Optical Networks (AONs)

While today's core optical switches continue to handle core grooming, the addition of all-optical (photonic) switches [14], [15] will even further expand the benefits of optical networking in the future. A unique property of a WDM all-optical network is the ability to do wavelength routing. Here, the path of the signal through the network is determined by the wavelength and origin of the signal, as well as the states of the network switches and wavelength changers. Unlike other all-optical approaches, wavelength routing provides a transparent semi-lightpath between network terminals. This transparency provides a simple way for heterogeneous users to share network resources. For example, certain wavelengths could carry analog signals with other wavelengths simultaneously being used for digital. Moreover, different network terminals may use different modulation formats and terminals may be upgraded without any network reconfiguration. As a philosophy, the network will provide bandwidth on demand and let the users determine their individual hardware requirements.

There is a wide range of potential applications for the AON. In the near term, most of these applications can be individually supported by electronic networks. However, the aggregation of many services and the cost, quality-of-service, flexibility, and transparency supported by AON technology may prove superior to electronic networks. Interoperable all-optical switch elements will be added at nodes with today's intelligent optical switches (opaque) to handle an increasing number of 10 Gb/s signals at core rates and also to support the introduction of higher rate signals such as 40 Gb/s. This important next-generation network resource will provide carriers with new opportunities for cost reduction, the strength of a best-of-breed interoperable core and the introduction of new wavelength-based services.

3.3.5.9.1 Architecture

The architecture of an AON is very much similar to the architecture of modern computer networks and has been designed in a very structured way [4]. The architecture of AONs are organised as a series of layers. Each layer performs certain functions and offers certain services to its higher layer. The AON protocol layers can be defined as: i) Physical layer, ii) Optical layer, iii) Data link layer, iv) Network layer, v) Transport layer, vi) Session layer, vii) Presentation layer, and viii) Application layer. Introduction of "all-optical" networks greatly simplifies the communication as well as network control functions. As a result, several atomic functions will be executed once on behalf of the application only. Additionally, WDM networks use circuit switching and offer high degree of protocol transparency.

For all-optical local and metropolitan area networks, Green [4] suggested the deletion of network layer and data link layer from the conventional network architecture and assumed that the optical functions will be performed at the physical layer itself. He emphasised for a multi-access control layer at level 2 for the sake of simplification of control point function. On the other hand, for wide area backbone AONs, Introduction of optical network layer between data link layer and physical layer in optical network architecture will greatly simplify the network control functions. Lightpath assignment, wavelength routing, etc. will be the prime responsibility of optical layer. In all-optical networks, optical line terminal equipment (OLTE) forms the physical layer interface. Its function is to transport bits from one process to other through a fiber optic communication media in PDH/SDH/SONET/ATM networks using PDH/SDH/SONET/ATM frame formats or protocols.

3.3.5.9.2 Optical Layer Functions

The function of an optical layer is to provide services to data link layer (for example, ATM layer). The principal services that an optical layer offers to its higher layer are:

i) to set-up and takedown of lightpath (unidirectional or bi-directional) in order to transfer data from data link layer of the source node to data link layer of destination node through physical layer,

ii) to provide wavelength routing at intermediate nodes,

iii) to guarantee the required level of quality of service (QOS), and

vi) to ensure proper network management.

The communication between data link layer and optical layer uses *request*, *indication*, *response*, *confirm*, *set-up*, *set-up acknowledge*, *set-up confirm*, and *takedown* as primitives. The primitives can be defined as:

- lightpath request (source address, optical port address (source), destination address, optical port address (destination), QOS, directivity of lightpath, wavelength).
- lightpath indication (source address, optical port address (source), destination address, optical port address (destination), QOS, wavelength, direction).
- lightpath response (source address, optical port address (source), destination address, optical port address (destination), QOS, wavelength).
- lightpath confirm (source address, optical port address (source), destination address, optical port address (destination), QOS, wavelength).
- lightpath negative acknowledgement (source address, optical port address (source), destination address, optical port address (destination), QOS, wavelength).
- lightpath set-up (source address, optical port address (source), destination address, optical port address (destination), QOS, wavelength, single or multi hop).

- lightpath set-up acknowledgement (source address, optical port address (source), destination address, optical port address (destination), wavelength).
- lightpath set-up confirms (source address, optical port address (source), destination address, optical port address (destination), QOS, wavelength).
- lightpath takedown (source address, optical port address (source), destination address, optical port address (destination), wavelength).

Here, we define the terms *source address* as the address of the originating node wherefrom the lightpath originates, *destination address* as the address of the node to which the lightpath terminates, *optical port address* (*source*) as the address of the optical port which will be assigned for the lightpath set-up, and *optical port address* (*destination*) as the address of the optical port which will be assigned for the lightpath termination at the destination node. The term wavelength is being defined as the wavelength to be assigned to a particular lightpath. Directivity of lightpath defines the nature of the lightpath connectivity, i.e. whether it is unidirectional or bi-directional. QOS defines the quality of service of the proposed link or of the existing established link. The point-to-point link can be defined as a single hop, or multi-hop. In multi hop link, there exists intermediate node(s) with or without wavelength routing switch(s).

3.3.5.9.3 Control Protocol

Control protocol provides communication interface between optical layer and network management and control points [14], [15]. It is necessary to have a robust protocol interface between optical layer and network management and control layer for optimum network performance. Network control normally performs the function of setting up and taking down of lightpaths, and also rerouting of lightpaths in case of failure. We briefly introduce the topics here; details can be found in Chapter 6, where IP-over-WDM is described.

In a distributed network control of an all-optical network, switching nodes are connected by wavelength division multiplexed fiber optic links. No two connections in a link can be assigned with the same wavelength. A controller controls each node. Controllers communicate with each other over an inband or out-of-band communication network. In order to establish a new connection between two nodes, following operations are to be performed:

1. *Wavelength and route determination*: The source node has to determine the route and wavelengths from the topology database and wavelength usage database, which are to be updated time to time using topology update protocol.

2. *Reservation*: Source node generates requests to all controllers on the path requesting reservation of the corresponding wavelengths. This process is denoted by the event LightPath Request (LPR). After receiving request, each controller sends either a positive acknowledgement or a negative acknowledgement, and the positive acknowledgement event is denoted by the event LightPath Confirm (LPC), and LightPath Negative Acknowledgement (LPNA) denotes negative acknowledgement event.
3. *Connection set-up/release*: If the reservation process is successful, originator sends connection set-up message to all controllers for establishing lightpath between source and destination nodes. This event is denoted by LightPath Set-up (LPS). All the controllers will send set-up acknowledgement messages to originator, and the event is denoted by LightPath Set-up Acknowledgement (LPSA). When the originating node receives LPSA, it starts using connection and sends Lightpath set-up confirm (LPSC) to the destination node, informing it to use the connection. Similarly, takedown process will release connection between source and destination node when the connection is no more required and is denoted by the event LightPath Takedown (LPTD). Lightpath takedown may be of two types:
   - Originating node sends takedown messages to each controller in the lightpath, requesting them to release lightpath.
   - Each controller sends to each neighbouring controllers a list of wavelengths, and the state of all connections at that node. On receiving this message, neighbouring controller checks its own configuration table for the related entries and if no match is found, the lightpath connection will be released.

During establishment of lightpath, higher layer determines the Quality of service (QOS) for the lightpath. The parameters that are relevant for lightpath establishment which optical layer will provide to higher layer are as follows: Degree of transparency, Line bit rate, Type of modulation, Level of back up required/provided, Bandwidth, Required bit error rate/SNR, End to end delay on the lightpath and its backup lightpath, Jitter requirements for transport network, and security issues.

Now, from the implementation aspects of optical network architecture, a set of assumptions required to be made for the sake of simplification of the standards. These assumptions, however, may vary from one implementation to another. Most assume low set-up rate, isolation from physical layer and routing of bi-directional lightpaths. As higher level protocols use the lightpath as a physical layer, it is assumed that the set-up and take down of the lightpath will be infrequent. This leads to more simplified network control function. It is assumed that two unidirectional lightpath should follow the same physical route and same wavelength propagated in the opposite directions. This restriction simplifies the connection management during failure. To solve the routing and wavelength assignment problem, it is further assumed that physical layer constraints can be further simplified by putting constraints on the maximum number of routes.

3.4 WIRELESS BACKBONE NETWORKS

Wireless communication predates the Internet. But it was restricted to military communication mostly in its early days. With the advent of cellular technology, it has made a dramatic comeback in a new form to support user mobility.

3.4.1 Terrestrial Microwave Networks

Microwave networks [16] are a wide area communications system that uses the microwave end of the electromagnetic wave spectrum as a transmission medium. It is one of the oldest wireless backbone networks in use even today. It will certainly exist in PervNet too.

Microwave transmissions take place in the 3 to 30 GHz range of the electromagnetic spectrum. Terrestrial microwave networks operate over distances of up to 30 miles, between pairs of transmitting and receiving antennas, although the higher the frequency of transmission, the shorter the distance across which transmission can be made. Microwave transmission is traditionally being used for long distance television and telephone trunk transmissions. Such transmission was largely analogue, and it was only in the 1980's that digital techniques were widely adopted. Typically, a single 30 MHz section of microwave spectrum will be used to carry some 45 Mbits/s of digital data. Microwave networks are a very convenient way of moving relatively high bandwidth data across short distances, and are less costly to install than cable systems. One of the most common current applications is to provide data links between mobile phone cells (the transmitter/receiver at the heart of a geographical call) and telecommunications switching centres [18].

In order for microwave antennas to achieve clear transmission they must be an uninterrupted line-of-sight between pairs. At the midpoint between the transmitter and receiver, the beam can spread in diameter up to a few dozen metres and this area, known as the *Fresnel Zone*, must be completely clear of obstructions such as trees, buildings, or hills. The maximum distance between microwave transmitters is dictated principally by the curvature of the earth, although atmospheric conditions tend to mean that distances less than the theoretical limit are chosen for transmitter receiver pairs for the practical purpose of guaranteeing throughput in the majority of weathers. Water, in the form of humid air, fog or rain absorbs microwave energy and can disrupt transmissions. Microwave communications over long distances are achieved by the use of series of microwave repeaters, which receive, re-amplify and retransmit a signal to the next post.

Microwave networks are used to provide a high bandwidth network infrastructure for broadcast transmission (television) and long distance two-way communication (voice and data). Increasingly digital microwave transmissions are being used to provide a digital bypass for congested cable networks in order to cope with massive bandwidth requirements. Finally microwave transmission is the basis of all satellite communications [17], be it video, voice or data. Microwave networks are capable of supporting data intensive applications such as real-time video transmission. Microwave networks are probably most commonly used for television broadcasts between regional relay transmitters, where the signals are then re-broadcast on longer wavelength radio frequencies. Microwave networks can provide a digital bypass for the optical fibre and cable based networks in PervNet. On the negative side, microwave transmission requires 'line of sight' between transmitters, which restricts their application in urban areas. Microwave transmission is susceptible to atmospheric interference including rain absorption (the rain drops are heated up as they absorb microwave radiation). Microwave transmissions are hazardous to health and care is needed to ensure that humans and animals do not intercept a microwave beam near its source.

3.4.2 Satellite Networks

Satellite communications [17] play an important role in providing access to communication services at the global level, and it has become quite evident there has been a significant increase in the use of satellite technology for commercial purposes over the past decade. Satellite use is expected to continue to escalate in PervNet. Microwave is the basis of satellite communications; earth stations transmit data to satellites, which receive, re-amplify and re-transmit the information to a geographically remote earth station.

Besides the general spectrum management principles, satellite licensing involves two additional principles: efficient use of the orbit spectrum resource and open skies. Given that the orbit spectrum is limited, the FCC has adopted policies and rules requiring its efficient use. The purpose of this policy is to facilitate licensing of the maximum number of systems possible, with minimal amount of interference. This approach is beneficial for consumers because it also facilitates competition, and provides a greater variety of services at the lowest possible prices. Through its satellite licensing policies, the FCC has increased the ability of licensees to adjust to a dynamic environment (as anticipated in PervNet). Except for limitations created by insufficient amounts of available spectrum, the FCC avoids imposing artificial limits on the number of commercial operators or the types of services they can offer. For example, early satellite systems carried mostly long-haul telephone transmissions. When fiber optic cable became prevalent, satellite licensees began to focus on other services, such as high-speed data and video services, as well as on providing both domestic and international service. A regulatory approach of flexibility has allowed the industry to thrive despite shifts in customer requirements. In accordance with the principles of its Open Skies policy, the FCC has licensed private companies that provide a wide range of satellite services. For example, in addition to licensing fixed-satellite services, the FCC has licensed mobile satellite services [18], direct broadcast services, radio determination satellite services, and remote sensing satellite services. These have included both geo-stationary and non-geo-stationary systems.

In addition to licensing the space station segment of the satellite system, the FCC is responsible for licensing earth stations. A satellite earth station is defined as a complex of transmitters, receivers, and antennas used to relay and/or receive communications traffic (voice, data, and video) through space to and from both satellites in geostationary satellite orbits (GSO) and non-geostationary satellite orbits (NGSO). The predominant bands for earth station transmissions are the C-band, the Ku-band [17] and Ka-band for fixed satellite services, and the 1.6/2.4 GHz bands and the 137-138/148-149.9 MHz bands for mobile satellite service [18].

The FCC rules for earth station licensing are contained in part 25 of Title 47 of the Code of Federal Regulations. There are several classes of earth stations-Fixed Earth Station (transmit/receive), Temporary-Fixed Earth Station (non-permanent, transportable, transmit/receive), Fixed Earth Station (receive-only), Fixed Earth Station (VSAT Network, 12/14 GHz), Developmental Earth Station (fixed or temporary-fixed), and Mobile Earth Station (hand-held units and vehicle-mounted units). Such earth stations may be used for domestic and/or international services. Earth stations are usually licensed for a specific period (say, in the United States, generally, for a period of 10 years), except for Developmental Earth Stations, which are licensed for one year. All earth station licenses are subject to renewal by the FCC. Earth stations must meet certain technical requirements before they can be authorized. These technical system parameters include: antenna performance standards, antenna size, environmental impact (including radiation hazard standards), Radio Frequency power conservation (EIRP and

EIRP density), modulation formats, and antenna structure heights. The FCC also issues a single blanket license for large number of technically identical earth stations (*e.g.*, VSATs, SNG and Mobile earth stations [18]). The number of terminals per application is not limited by the FCC, but is independently requested by the applicants. Any modifications to a transmitting earth station also require prior authorization.

A significantly more effective, economical approach to time-essential data networking is with solutions that use satellite and VSAT technology. VSAT is an acronym for Very Small Aperture Terminal. The word terminal is used interchangeably with the words antenna and station. A VSAT network consists of two major components, a ground segment and a space segment. The ground segment consists of a central hub station and a family of remote terminals (satellite earth stations) generally referred to as remote VSATs. The space segment consists of the satellite and its on-board transponders. Hub stations use larger antennas (greater than 3.0-meters in diameter). VSAT stations use smaller size antennas (1.2-meters, 1.8-meters, and 2.4-meters). Most VSAT networks in the United States are constructed/licensed in the Ku-band [17], 14000-14500 MHz (uplink) and 11700- 12200 MHz (downlink), while a limited number of C-band VSAT networks have been licensed. Reliable, scalable and easy to deploy, VSAT-based networking solutions enable the reliable delivery of mission-critical data, video and audio content, across town or around the globe. VSAT networks can be deployed in a small part of the time and managed with a fraction of the staff required by terrestrial systems- a valuable proposition in today's downsized work environment.

There is a need to develop an architectural framework for satellite networks, within which information-based PervComp applications can realize their full potential. Also, a framework will be useful for standards, experiment design, and strategic planning for satellite networks. Satellite Networks and Architecture branch of NASA is developing approaches to frameworks based on end-users, enterprise networks, service providers, and satellite network operators. They also participate in discussions about the architecture frameworks being developed by various standards-making bodies (ITU, ANSI, ATM Standards, etc.) and their pros and cons. From this foundation of cooperation, research, and development, they will answer the need for a higher-level systems engineering approach for development of architectural framework for the next-generation satellite networks in PervNet.

3.4.3 Wireless (Fibreless) Optical Networks

We know that optical systems using laser links have the ability to communicate between two fixed points separated by a line-of-sight (LOS) path through the atmosphere, with large available bandwidth without the requirement for licensing inherent in deploying radio or microwave systems. Since this does not involve any cabling, it is known as free space optics (FSO), or fibreless optics or *optical wireless* (OW) communication. OW is an attractive alternative to traditional terrestrial Radio Frequency (RF) wireless. OW systems can be densely deployed in urban areas without incurring interference problems. They can offer much higher capacities than RF systems, require no licensing, and can be very cost-competitive. OW systems work on a line-of-sight, point-to-point basis and have ranges extending up to and beyond 2 km (1.25 miles).

Terminals need not be deployed outdoors- they can be set up in an office by a window. The only requirement is a clear view of the other end of the link. After the beam leaves the terminal, it spreads out. Systems with a beam-spread of half a degree or less can be used, but alignment will be upset by building movements caused by winds unless active auto-tracking is used. Systems with larger beam spreads are more immune to building shake but have lesser range.

OW can be used between buildings and campuses using portable terminals for high-data rate (hundreds of Mbps) links. For instance, high-speed digital data networks can be connected through the atmosphere using point-to-point light beams. It can be used for accessing the Internet backbones, transfer of medical, banking, and computer data, and other applications where high-data rate links are needed with minimum FCC or local government regulation, and where infrastructure investment is not committed to a specific building or city. Thus, it has huge potential in ad hoc PervNet deployment. ISPs are already using OW solutions to provide high speed Internet access directly to their clients with minimal planning or installation delays. Some OW systems use Light-Emitting Diodes (LEDs), which are safer and more reliable than lasers. This greatly reduces the costs of preventive or corrective maintenance. The LED based systems are also much less of a threat to the eyes, producing power densities on the retina 1,000 times less than those from lasers. They can safely be viewed at close range or through binoculars.

The huge benefits of FSO technology include immense bandwidths previously obtainable only over fibre-optic cable, genuine 'cable-free' point-to-point connection, and freedom from stringent radio licensing regulations. Data networks, which are separated by a clear line-of-sight path up to and exceeding 1 kilometre, can be connected with an installation that typically takes 2-3 hours, overcoming traditional limitations of electrical cable, fibre-optic, microwave, or leased-line systems. OW networks promise transmission without interference, and promise to provide higher security, simply because the transmission involves a beam rather than a radiated signal. The beams are so well confined and high in the air that any interception operation is very exposed and liable to disrupt transmission in a very obvious way, warning system managers. OW systems are basically free of interference; many terminals can be located close together on the same rooftop. This contrasts with the RF radio situation where great care has to be taken with deployment and frequency re-use to minimize interference, and the task is almost impossible in urban areas using the unlicensed RF bands.

There are two major issues for OW: fog and direct sunlight. Direct sunlight is only a problem if the link is on an East-West line. It may disable one receiver for a minute or two during dawn and dusk. Fog, however, can be real problem, and OW systems should not be deployed in areas where thick fog is a frequent occurrence. Rain, snow, and light fog are not major problems, as OW systems are all designed with sufficient margins to cope with these effects.

OW is an excellent choice for large institutions with specific point-to-point needs, such as a university that needed to cross a government-owned highway that cut through the campus, and could not get permission to dig. The university can then use an OW connection between two science buildings to complete its network. Products are already available in the market for GSM [18] providers and ISPs. These links enable customers to transmit data at Ethernet speeds while still accessing alternate lines, essentially allowing a user to access phone lines and Ethernet data transmission over the same link. Some more typical application scenarios that may appear to ensure connectivity in PervNet are:

- Separate office blocks, each with. corporate data networks (e.g. Ethernet, Token Ring, ATM), which need to be connected. The ground between premises is either public property or cannot be excavated. Conventional leased-lines are expensive or lack high-speed (>100 Mbps) performance.
- Installing PervNet infrastructure in developing countries typically involves terrestrial microwave links between cities; but licensing, interference and reflections from buildings prohibit the use of microwave to connect the central city telephone exchange(s) to the nearest microwave tower. Digging up the city streets to install cables is expensive, slow and causes disruption.
- PervNet needs on-site data communications between computers in temporary buildings or vehicles to facilitate management of a large and complex project. Cables would be broken by passing vehicles and would

need moving frequently, and licenses for radio or microwave systems might not be granted for mobile use or in all regions.

- Location tracking may involve many TV cameras connected to each other. Conventionally, this requires kilometres of cable and days of installation time. The event may take place in a country where licensing for microwave links cannot be obtained quickly, the spectrum is overcrowded or interference likely.
- PervNet requires cost-efficient backup links either between buildings or between the satellite earth terminal to avoid 'down-time' and consequent breaks in transmission. In a PervNet environment, maintenance to the main system may regularly require use of the backup.
- Commercially sensitive or governmental/military operations require data links which cannot easily be intercepted and not without the knowledge of the operator. The near-impossibility of partially-intercepting the narrow beam of an optical system without break in the original transmission path or without radical change in received signal level is a major benefit of FSO transmission technology.

3.5 THE INTERNET

Combining all the above technologies into a single PervNet backbone is a viable proposition because there is already a precedence called the Internet [1]. The technological marriage between computer and communication in early 70's giving birth to the new industry called computer networking is now a glorious history. The most famous offspring of this family, the Internet has already shown us the way to integrate differing technologies under a single broad umbrella. Apart from technological spin-offs, it has also triggered off a number of social, economical and technological revolutions in the last decade. All these indicate that PervNet is on its way; it could be the next evolutionary step for the Internet itself.

The Internet is based on two protocols: Transmission Control Protocol (TCP) and Internet Protocol (IP). They are a pair of protocols that allow one subnet to communicate with another [1]. As previously mentioned, their operation should be transparent to the Physical and Data Link layers and can thus be used on Ethernet, FDDI or Token Ring networks. The address of the Data Link layer corresponds to the physical address of the node, such as the MAC address (in Ethernet and Token Ring) or the telephone number (for a modem connection). The IP address is assigned to each node on the Internet and is used to identify the location of the network and any subnet.

TCP/IP was originally developed by the US Defense Advanced Research Projects Agency (DARPA). Their objective was to connect a number of universities and other research establishments to DARPA. The resultant internet is now known as the *Internet*. It has since outgrown this application and many commercial organizations and home users now connect to the Internet. The Internet uses TCP/IP as a standard to transfer data. Each node on the Internet is assigned a unique network address, called an IP address. Note that any organization can have its own internets (called intranets), but if it they want to connect these to the Internet then their addresses must conform to the Internet addressing format.

TCP/IP hosts are nodes, which communicate over interconnected networks using TCP/IP communications. A TCP/IP gateway node connects one type of network to another. It contains hardware to provide the physical link between the different networks and the hardware and software to convert frames from one network to the other. Typically, it converts a Token Ring MAC layer to an equivalent Ethernet MAC layer, and vice versa [1]. A router connects a network to another of the same kind through a point-to-point link. The main operational difference between a gateway, a router, and a bridge, is that, for a Token Ring and Ethernet network, the bridge uses the 48-bit MAC address to route frames, whereas the gateway and router use the IP network address. As an analogy to the public telephone system, the MAC address is equivalent to a randomly assigned telephone number, whereas the IP address would contain the information on the logical located of the telephone, such as which country, area code, and so on. The gateway reads the frame from the computer on network A. It then reads the IP address contained in the frame and makes a decision as to whether it is routed out of network A to network B. If it does then it relays the frame to network B.

The areas of modern life that have more jargon words and associated acronyms than anything else are the World Wide Web (WWW) and the Internet. The WWW was initially conceived in 1989 by CERN, the European particle physics research laboratory in Geneva, Switzerland. Its main objective was: *to use the hypermedia concept to support the interlinking of various types of information through the design and development of a series of concepts, communications protocols, and systems.* One of its main characteristics is that stored information tends to be distributed over a geographically wide area. The result of the project has been the worldwide acceptance of the protocols and specifications used. A major part of its success was due to the full support of the National Center for Supercomputing Applications (NCSA), which developed a family of user interface systems known collectively as Mosaic. The WWW, or Web, is basically an infrastructure of information. This information is stored on the WWW on Web servers and it uses the Internet to transmit data around the world. These servers run special programs that allow information to be transmitted to remote computers, which are running a Web browser. The

Internet is a common connection in which computers can communicate using a common addressing mechanism (IP) with a TCP/IP connection. The information is stored on Web servers and is accessed by means of pages. These pages can contain text and other multimedia applications such as graphic images, digitized sound files and video animation.

Each page contains text known as hypertext, which has specially reserved keywords to represent the format and the display functions. A standard language known as HTML (Hypertext Markup Language) has been developed for this purpose. Hypertext pages, when interpreted by a browser program, display an easy-to-use interface containing formatted text, icons, pictorial hot spots, underscored words, and so on. Each page can also contain links to other related pages. The topology and power of the Web now allows for distributed information, where information does not have to be stored locally. To find information on the Web, a user can use powerful search engines to search for related links. For example, the user initially accesses a page on a German Web server, this then contains a link to a Japanese server. This server contains links to UK, Swedish and French servers. This type of arrangement leads to the topology that resembles a spider's web, where information is linked from one place to another.

The WWW and the Internet tend to produce a polarization of views. Thus, before analysing the WWW for its technical specification, a few words must be said on some of the subjective advantages and disadvantages of the WWW and the Internet. It should be noted that some of these disadvantages can be seen as advantages to some people, and vice versa. For example, freedom of information will be seen as an advantage to a freedom-of-speech group but often a disadvantage to security organizations. The WWW is structured with clients and servers, where a client accesses services from the server. These servers can either be local or available through a global network connection. A local connection normally requires the connection over a local area network but a global connection normally requires connection to an Internet provider. These providers are often known as an Internet access provider (IAPs), sometimes as an Internet connectivity provider (ICP) or Internet Service Providers (ISPs). They provide the mechanism to access the Internet and have the required hardware and software to connect from the user to the Internet.

The 21st century is the age of *Internet* (main component of PervNet backbone) and *World Wide Web* (basis for PervComp applications). The Web is revolutionizing the way we gather, process, and use information, leading to PervComp. At the same time, it also redefines the meanings and processes of business, commerce, marketing, finance, publishing, education, research, development, as well as other social aspects of our daily life. Although individual Web-based information systems are constantly being deployed, advanced issues and techniques for developing PervComp applications still remain to be systematically studied (as hinted in chapter 1). TCP/IP will be the architecture of most upcoming networks so that they can be easily connected to the Internet. Pervasive IP is the focus of all attention because its success will define a number of related parameters and will solve many unresolved issues in a single stroke. We will learn more about the Internet in Chapter 6.

3.6 SUMMARY

The concept of PervNet is to provide access to a set of communication services that is an open multitude of information-based applications and services, to everyone, every time, everywhere at acceptable cost and quality. This can be achieved by the seamless interconnection of all networks, information systems, and applications. The bourgeoning business and consumer appetite for the core networks (such as the Internet), coupled with demands for virtual private networks and other new services such as PervComp, is driving bandwidth requirements for the backbone to the limits of today's communications systems. With the rapid spread of multimedia PervComp applications leading to an exponential growth in PervNet traffic, backbone networks are clearly on the threshold of a new era. As a result, backbone service providers, as well as the incumbent carriers, are racing to expand their network infrastructure effectively because PervComp is aiming to offer consumers and businesses with choices that they had never experienced before. As usual, users are always in search of more and more bandwidth that sophisticated PervComp services are asking for. The rapid growth of PervNet traffic is also increasing the need for long haul capacity at a fast pace. With the PervNet, you are as likely to be sensing an event that is happening half way across the country, as one that is happening locally. Supporting these new-world, bandwidth-hungry applications in PervNet requires a backbone network characterized by rapid point and click provisioning, QOS based restorations, and a least-cost-per-bit mindset. Moreover, the exponential growth in backbone traffic and increasingly unpredictable demand patterns make the need for a scalable architecture for the backbone of PervNet paramount.

Of late, fiber optic systems are being widely used for establishing communication networks throughout the world because of its high bandwidth and very low received bit error rate. Due to this technological revolution, from 1970's to now, data communication has evolved from 56 Kbps (ARPANET) to 10 Tbps (modern optical communication), a gain of more than a factor of 100 per decade. At the same time, error rate went from

10^{-5} per bit to almost zero in fibre optics. Accordingly, there is a recent trend for the development of wide area optical networks in order to take advantage of the tremendous bandwidth potential of fiber optic cables. Several projects, such as AON, MONET, NTON, ACTS-HORIZON [2]-[5], [14],[15] are evidences of this fact. Availability of optical amplifiers has opened up a new avenue for multiplexing many wavelengths in the same fibre. Fortunately, the spread of optical networks from long-haul to metropolitan rings and now to customer premise locations, is creating an ocean of bandwidth for carrier core networks. Optical WDM networking technology is spearheading a bandwidth revolution in the infrastructure of the next generation Internet and beyond (i.e., PervNet). Demand for bandwidth is rapidly increasing with the possibility of new kinds of applications such as electronic commerce, video on demand, global cooperative work, and PervComp.

Optical WDM networks offer tremendous promise in meeting this demand. The basic concept of WDM technology is the ability to simultaneously transmit data on multiple wavelengths on a single fiber. WDM provides a practical solution to the *optoelectronic* speed mismatch problem. This mismatch arises since the theoretical capacity of fiber optics is close to 75 Tbps, while current electronic processing is limited to a few Gbps. With WDM, several independent channels each operating at a few Gbps are created– a speed that is within electronic processing limits. The theoretical upper limit on the number of channels is close to one thousand, which has been recently achieved in laboratory demonstrations at Lucent Technologies. However, the rapid growth of PervComp, together with newer applications and services make it imperative that this bandwidth be quickly and effectively harnessed.

REFERENCES

[1] Buchanan B., Handbook of Data Communication and Networks, Kluwer Academic Publishers, 2000.

[2] Mukherjee B., Optical Communication Networks, McGraw-Hill, New York, 1997. Ramaswami R. and Sivarajan K., Optical Networks: A Practical Perspective, Morgan Kaufmann Publishers, 1998.

[3] Green P. E., "Progress in Optical Networking", IEEE Communications Magazine, pp. 54-61, January 2001.

[4] Mukherjee B., "WDM Optical Communication Networks: Progress and Challenges", IEEE Journal on Selected Areas in Communications, Vol. 18, No. 10, pp. 1810-1824, October 2000.

[5] Dutta R., and Rouskas G. N., "A Survey of Virtual Topology Design Algorithms for Wavelength Routed Optical Networks", Optical Networks Magazine, Vol. 1, no.1, pp. 73-89, January 2000.

[6] Zang H., Jue J. P. and Mukherjee B., "Review of routing and wavelength assignment approaches for wavelength-routed optical WDM networks", Optical networks, Vol. 1, no.1, pp. 47-60, Jan. 2000.

[7] Saha D., and Sengupta D.,"An optical layer lightpath management protocol for AONs", Photonic Networks & Communication, Vol.2, No.2, pp. 185-198, 2000.

[8] Saha D.,"Forward reservation protocol with immediate unlock (FRP-IU) for dynamic establishment in all-optical networks AONs", Proc. SPIE Terrabit Optical Networking, Boston, USA, Nov. 2000.

[9] Saha D., "An efficient wavelength reservation protocol for lightpath establishment in all-optical networks (AONs)", Proc. IEEE GLOBECOM'2000, San Fransisco, USA, Nov/Dec. 2000.

[10] Saha D.," A Comparative Study of Distributed Protocols for Wavelength Reservation in WDM optical networks", Optical Networks Magazine, Vol. 3, No. 1, SPIE, USA, 2002.

[11] Zhang Z. and Acampora A. S., "A Heuristic Wavelength Assignment Algorithm for Multihop WDM Networks with Wavelength Routing and Wavelength Re-Use", IEEE/ACM Transactions on Networking, Vol.3, No.3, pp. 281-288,June 1995.

[12] Saha D. et. al,"An approach to wide area WDM optical network design using genetic algorithm", Computer Communication, vol.22, (Jan 1999), pp.156-172.

[13] Sivalingam K, and Subramanium S, (Ed.) Optical WDM Networks, Kluwer Academic, 2000.

[14] Ramamurthy B, Design of Optical Networks, LAN, MAN and WAN Architectures, Kluwer Academic, 2001.

[15] Janaswamy R, Radiowave propagation and Smart Antennas for Wireless Communication, Kluwer Academic, 2000.

[16] Lee C-H, and Laskar J, Compact Ku –Band Transmitter- Design for Satellite Communication Applications, Kluwer Academic, 2002.

[17] Stuber G. L., Principles of Mobile Communication, 2nd Ed., Kluwer Academic, 2001.

Chapter 4

Wireless Access Technology

As discussed in Chapter 2, access in PervNet will preferably be wireless to accommodate end-user mobility. After learning backbone technologies, those will be used in PervNet, in the previous chapter, the focus is now on the wireless access technologies that may find places in PervNet.

4.1 INTRODUCTION

Recent progress in wireless technologies provides clear indications that wireless access can be used to build cost-effective, easily deployable, high-speed digital telecommunication network of the future. In particular broadband wireless access technology would provide a scalable and affordable access solution that supports data, voice, video as well as connectivity to the Internet. At the same time, the users may need to access the global telecommunication infrastructure or may need to communicate with any other user anywhere in the globe, even when they are mobile and away from their home-base. Thus, there are two major motivations behind the growth of wireless access technologies: *Fixed Wireless Access* and *Mobile Wireless Access.*

4.1.1 Fixed Wireless Access

The objective here is to provide wireless access that is equivalent to a wireline access. This appears to the user and the service provider as a transparent equivalent to wireline service, and does not need to be differentiated. In many cases, for implementing a new network or introducing broadband accesses in an existing network, it would be more economical to implement wireless access solutions rather than deployment of cables. In these situations, the wireless solutions can also be implemented in a shorter period of time in comparison with an entire wireline solution, thus favoring the fast development of any country.

A network may be viewed as a set of nodes and links where the links connect the nodes. Nodes can be fixed or mobile and can be of two types: end-points (or terminals) and switches (or routers) [1]. Similarly, links also can be classified as two types: wireline and wireless links. Based on this taxonomy, the fixed wireless access network can be described as a network with wireless link between fixed end-point and fixed switch (e.g. cordless telephony), between two fixed switches (e.g. microwave links between two switches) or between two fixed end-points (e.g. short-range radio connectivity between a computer and a printer). This configuration supports limited mobility i.e the end-point may move keeping its link intact with the switch or another end-point. For example, the user can roam within his room with his cordless phone. However, there is no need to manage the mobility or to track the location of the user. In other words, even if the nodes may move in this configuration, the link between them has to be fixed or has to remain intact in order to provide a fixed access between them. That is why this configuration is treated as fixed access, even if it supports limited node mobility.

4.1.2 Mobile Wireless Access

Mobility is the key issue here. From the networking point of view, there are two types of configurations. Wireless connectivity between mobile end-point and fixed switch while the mobile end-point is allowed to move freely and change its association from one switch to another. The major goal here is to allow a user to have access to the capabilities of the global network or to another user at any time without regard to its location or mobility. The cellular system is an example in this category. The cellular architecture requires single hop wireless connectivity to the wired network and this is achieved by installing fixed base stations and access points. In such networks, communications between two mobile end-points completely rely on the wired backbone and the fixed base stations. The mobile end-point is only one hop away from a base station and uses wireless links to get connected to the base station. A mobile terminal in this network connects to, and communicates with, the nearest base station that is within its communication radius. As the mobile travels out of range of one base station and into the range of another, a handoff occurs from the old base station to the new, and the mobile is able to continue communication seamlessly throughout the network. The ultimate objective here is global roaming with portable handset and ubiquitous access to voice/ video/ data of the global network together with multimedia communication with other users at any remote corner of the globe.

Another category is wireless connectivity between mobile end-points and mobile switches. The example is an ad hoc infrastructure-less network [2]. Infrastructure-less networks have no fixed gateways (routers); all nodes are capable of movement and can be connected dynamically in an arbitrary manner. Nodes of these networks function as routers, which discover and maintain routes to other nodes in the network. Applications of ad hoc networks include military tactical communication, emergency relief operations, commercial and educational use in remote areas, in meetings, etc. where the networking is mission-oriented and / or community-based. In such situations, an ad hoc network can be formed. An ad hoc network is a temporary network, operating without the aid of any established infrastructure of centralized administration or standard support services regularly available on the wide area network to which the hosts may normally be connected [2]. In these situations, no wired backbone infrastructure may be available for use by a group of mobile hosts. Also, setting up of fixed access points in these situations may not be a viable solution due to cost, convenience and performance considerations. Still, the group of mobile users may need to communicate with each other and share information between them. A message transfer in an ad hoc network environment would either take place between two nodes that are within the transmission range of each other or between nodes that are indirectly connected via multiple hops through some other intermediate nodes.

To structure our discussion on wireless access technology, we have divided the domain into three categories based on coverage area:

- Short-range wireless networks, sometimes referred to as PANs (personal area networks), commonly using fixed-access wireless technologies
- Wireless LANs, which provide in-building, high-speed access over distances of 100 feet or more, using both fixed access and mobile access technology, depending on the configuration;
- Wireless MAN, covering a network that spans between a LAN and a wider WAN and commonly using fixed-access wireless technologies wireless WANs, representing next-generation cell-based mobile access data systems that potentially will provide global data mobility.

4.2 SHORT-RANGE WIRELESS NETWORKS (PERSONAL AREA NETWORKS)

The coverage area for a personal area network (PAN) is limited to small area and is used to communicate between proximal devices. Infrared technology, that has become so popular because of household wireless devices, may be viewed as a precursor to PAN. The reduced costs of such infrared devices also make them an attractive technology that has already been accommodated by most of the portable devices such as laptops, PDAs, etc. Serial infrared data communication has been on the computer market for several years. Standardization and consequently mutual understanding between different devices has been achieved by the creation of the IrDA (Infrared Data Association). Another alternative technology is short-range wireless radio-based networks that have become an active area of research during the past decade. To realize such a wireless radio access system vision, the mobile telephony and computing leaders Ericsson, IBM, Intel, Nokia, and Toshiba formed in February 1998 the Bluetooth special interest group. Bluetooth employs low power (1 mW), short-range (up to 10 m) radio transmission in the 2.4 GHz ISM frequency band and provides voice and asynchronous data services.

4.2.1 Basics of Infrared (IR) Access

The visible spectrum of electromagnetic radiation ranges from 400 nm (violet) to 700 nm (deep red). Wavelengths shorter than 400 nm are considered ultraviolet; those longer than 700 nm are considered infrared. While infrared radiation extends from 700 to 1,300 nm or longer, it is generally the so-called "near-infrared" region of 700 to 950 nm in which IR emitters and detectors operate.

IR links may employ various designs, and may be classified according to two criteria [3]. The first criterion is the degree of directionality of the transmitter and receiver. Directed links employ directional transmitters and receivers, where the transmitter should point towards receiver in order to establish a link. This can maximize power efficiency, since it minimizes path loss and is less affected by ambient light noise. Nondirected links employ wide-angle transmitters and receivers. Nondirected links may be more convenient to use, particularly for mobile terminals, since they do not require aiming of the transmitter or receiver. It is also possible to establish hybrid links, which combine transmitters and receivers having different degrees of directionality. The second classification criterion relates to whether the link relies upon the existence of an uninterrupted line-of-sight (LOS) path between the transmitter and receiver. LOS links rely upon such a path, while non-LOS links generally rely upon reflection of the light from the ceiling or some other diffusely reflecting surface. LOS link design maximizes power efficiency and minimizes multipath distortion. Non-LOS link design increases link robustness and ease of use, allowing the link to operate even when barriers, such as people or cubicle partitions, stand between the transmitter and receiver. The greatest robustness and ease of use are achieved by the nondirected-non-LOS link design, which is often referred to as a diffuse link [3].

Infrared emitters and detectors capable of high-speed operation are available at low cost. The infrared spectral region offers high bandwidth that is unregulated worldwide. IR transmissions are confined to the room in which they originate. This signal confinement and use of directional beam makes it easy to secure transmissions and it prevents interference between links operating in different rooms. However, this confinement is a drawback of IR communication and connectivity from one room to another requires the installation of IR access points that are interconnected via a wired backbone. Also, presence of sunlight, incandescent lighting and fluorescent lighting induces noise in an IR receiver.

The Infrared Data Association (IrDA) is an industry-based group of over 150 companies that have developed communication standards especially suited for low cost, short range, cross-platform, point-to-point communications at a wide range of speeds. These standards have been implemented on various computer platforms and more recently have become available for many embedded applications.

4.2.2 Infrared Communication Configurations

The most popular configuration for infrared communication is point-to-point communication between two nodes in a network. For example, two portable devices can communicate with each other using IR link for exchange of information. Another common application is to connect a laptop to the desktop using IR link to access the desktop applications or to take printouts of files in laptop from the printer connected to the desktop.

Using IR link, a portable device may be connected to an access point that is connected to a wired backbone, thus extending the range of connectivity. In a recent advancement on point-to-point IR link, the proposals for a new physical layer (PHY) and a modified link access protocol (LAP) were adopted as IrDA's new Very Fast Infrared (VFIr) standard. VFIr provides a channel data rate of 16 Mb/s, quadrupling the 4 Mb/s maximum of IrDA's widely implemented standard for wireless point-to-point communication. [4].

However, configuring IR multipoint is not so easily achievable. One example of realizing such configuration is called Advanced Infrared (AIr) [5]. AIr was developed within IBM including the IR group of the Zurich lab and other members of the Infrared Data Association (IrDA) to achieve the functionality needed to form multi-point network [6]. AIr allows a number of devices within 8 meters of each other to communicate without interference. Able to reliably connect one device to many or many to many at speeds of up to 4 Mb/s, AIr is well suited for supporting applications such as LAN access, shared whiteboards, multiperson games and ad hoc networking, in which people can sit down at a conference table and instantly form a wireless team within a room.

To ensure high-quality, inference-free communications, a major system change allows AIr's variable-rate transmission scheme [6] to work with a well-known wireless protocol. The idea is to ensure that each device has fair access to the medium without adding design complexity: A device that wants to transmit first reserves a short period during which everyone else is supposed to refrain from transmitting. But this does not always prevent interference. The problem is a lack of symmetry: in IR devices, the light-emitting diode (LED) transmitter and the photodiode receiver have different angular characteristics for emission and reception. In certain situations, this imbalance makes it possible for a device to miss the call for silence even though it is close enough to cause interference. The solution involves "parity", that is, in each device the sending power and the receiving sensitivity are matched so that the protocol can be reliably implemented. AIr achieves its highest data rates with a clear line of sight between devices. When such a direct connection is lost, a variable data rate scheme allows lower-speed communication with diffuse and reflected signals. The maximum speed for a given condition is automatically determined by counting the errors in a transmission. When the errors exceed a certain level, a signal is sent back to the transmitting device to slow its data rate.

4.2.3 Short-range Radio Communication

Radio and IR are complementary transmission media, and different applications favor the use of one medium or the other for short-range communication. Radio is favored in applications where user mobility must be maximized or transmission through walls or over relatively long ranges is required, and may be favored when transmitter power consumption must be minimized. Another advantage of using radio frequency for short-range communication over IR is that, it is not sensitive to ambient light condition. However, other types of interferences in communication are common, since it normally uses omni-directional antenna and not directed beam. Devices using similar frequencies - wireless phones, scanners, wrist radios and personal locators can interfere with transmission. It also has higher cost than infrared and data transmission rate is lower than wired and infrared transmission

Bluetooth is the most promising standard evolved to support short-range radio communication. Current capabilities of Bluetooth to support multimedia applications such as videophony are limited mainly due to the low maximum user data rate of less than 1 Mb/s in the 2.4 GHz band. Future short-range radio communication systems will likely overcome this limitation by being operated in the 5 GHz frequency band allowing data rates of 20 Mb/s and higher.

Bluetooth is based on a frequency hopping physical layer. So, the hosts are not able to communicate unless they have previously discovered each other by synchronizing their frequency hopping patterns. Thus, even if all nodes are within direct communication range of each other, only those nodes which are synchronized with the transmitter can hear the transmission. To support any-to-any communication, nodes must be synchronized so that the pairs of nodes (which can communicate with each other) together form a connected graph.

Bluetooth defines multiple channels for communication where each channel defined by a different frequency hopping sequence. A group of devices sharing a common channel is called a piconet [7]. Each piconet has a master unit which selects a frequency hopping sequence for the piconet and controls the access to the channel. Other participants of the group known as slave units are synchronized to the hopping sequence of the piconet master. Within a piconet, the channel is shared using a slotted time division duplex (TDD) protocol where a master uses a polling style protocol to allocate time-slots to slave nodes. The maximum number of slaves that can simultaneously be active in a piconet is seven.

Multiple piconets can co-exist in a common area because each piconet uses a different hopping sequence. Piconets can also be interconnected via bridge node to form a bigger network known as a scatternet [7]. Bridge nodes are capable of timesharing between multiple piconets, receiving data from one piconet and forwarding it to another. There is no restriction on the role a bridge node can play in each piconet it participates in. A bridge can be a master in one piconet and slave in another (termed as M/S bridge) or a slave in all piconets (termed as S/S bridge). However, Bluetooth normally supports point-to-point or point-to-multipoint configuration. Formation of multi-access networks using scatternet is a complex task and further investigations are needed for its success. For example, the reformation of an existing network in the face of dynamic changes is an important issue in this context. After network connection, a separate topology maintenance and optimisation protocol needs to run, in order to take care of mobility and/or nodes entering and leaving the network and make sure that the scatternet is reformed accordingly with minimal overhead [7].

4.3 WIRELESS LANS

Wireless LANs have become an extremely potential networking option with the acceptance of standards such as IEEE 802.11 (2 Mbps) and 802.11b (11 Mbps) in 2.4 GHz band. Companies are also trying for IEEE 802.11a with new technologies that are supposed to reach speeds of 54 Mbps in 5GHz band.

Wireless LANs have the ability to work in conjunction with wired networks or as a standalone technology. In the first technique, wireless links are used to achieve access to resources on a wired infrastructure. This wireless LAN architecture is well suited for wireless data communications in places, where the cost of installing a backbone and wireless access points can be justified. This configuration utilizes fixed wireless access points and the portables are connected to this access point using wireless links. So, the portables are one-hop away from an access point. The configuration is similar to a cellular network. The access point can also act as a bridge to a wired LAN, or, a set of access points can be connected to a base station that act as a bridge to a wired network, thus forming a larger network. However, communication over this kind of wireless LAN is controlled by the centralized controllers (access points or base stations).

The standalone wireless LANs, also called ad hoc networks or infrastructureless, multihop network, do not rely on centralized infrastructure. Ad hoc networks [2] are envisioned as infrastructure-less networks where each node is a mobile router, equipped with a wireless transceiver. A message transfer in an ad hoc network environment would either take place between two nodes that are within the transmission range of each other or between nodes that are indirectly connected via multiple hops through some other intermediate nodes. This is shown in Figure 4.1. Node C and node F are outside the wireless transmission range of each other but still be able to communicate via the intermediate node D in multiple hops. Similarly, node A and node G are outside the wireless transmission range of each other but still be able to communicate via the intermediate nodes C and D in multiple hops. However, since all nodes are mobile, it may so happen that C and D have gone out of range of each other, making the network separated into two isolated subnetworks for some time before other nodes come into rescue. There has been a growing interest in ad hoc networks in recent years and we will now discuss it in more details.

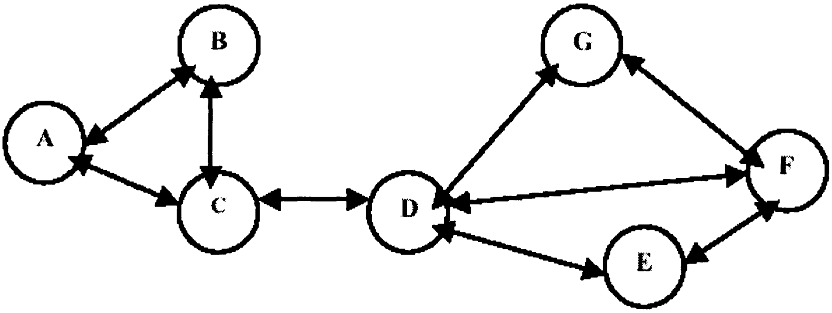


Figure 4.1 An Example Ad Hoc Network

4.3.1 Characteristics of Ad hoc Wireless Networks

Ad hoc Networks have several salient characteristics [2,8,9]:

Dynamic Topologies: Because of the possibly rapid and unpredictable movement of the nodes and fast changing propagation conditions, network information such as link-state, for example, becomes quickly obsolete. This leads to frequent network re-configurations and frequent exchanges of control information over the wireless medium.

Asymmetric Link Characteristics: In a wireless environment, communication between two nodes may not work equally well in both the directions. In other words, even if node n is within the transmission range of node m, the reverse may not be true. Although we have assumed bi-directional links in Figure 4.1, some of them may be unidirectional in a real-life scenario.

Multihop Communication: Each node in an ad hoc network will act as a transmitter, receiver or a relay station. So, packets from a transmitter node (source) may reach the receiver node (destination) in multiple hops through several intermediate relay nodes. However, the successful operation of an ad-hoc network will be hampered, if an intermediate node, participating in a communication between a source-destination pair, moves out of range suddenly or switches itself off in between message transfer. The situation is worse, if there is no other path between those two nodes. In Figure 4.1, if D moves out of range disconnecting the link between C and D, or if D switches itself off, the communication between C and F would be interrupted. Absence of D creates two disconnected components: {A, B, C} and {E, F, G}.

Decentralized Operation: Ad hoc networks are network architectures that can be rapidly deployed and that do not need to rely on pre-existing infrastructure or centralized control. In cellular wireless networks, there is a number of centralized entities; e.g., the base-stations, the Mobile Switching Centres (MSC-s), and the Home Location Registry. In ad hoc networks, since there is no pre-existing infrastructure, these centralized entities do not exist. The centralized entities in the cellular networks perform the function of coordination. Thus, lack of these entities in the ad hoc networks requires more sophisticated distributed algorithms to perform equivalent functions.

Bandwidth-constrained, Variable Capacity Links: Wireless links will continue to have significantly lower capacity than their hardwired counterparts. In addition, the realized throughput of wireless communications is often much less than a radio's maximum transmission rate because of the effects of multiple access, fading, noise, and interference conditions, etc. One effect of the relatively low to moderate link capacities is that, congestion is typically the norm rather than the exception. Thus, the aggregate application demand will likely approach or exceed network capacity frequently. This demand will continue to increase as multimedia computing and collaborative networking applications rise.

Energy-constrained operation: The mobile nodes in an ad hoc network rely on batteries or other exhaustible means for their energy. For these nodes, the most important system design criteria for optimisation may be energy conservation. One way of achieving this is to optimise the transmission power of each node.

These characteristics of ad hoc networks create a set of performance concerns for protocol design, which extend beyond those guiding the design of protocols for conventional networks with pre-configured topology.

4.3.2 Three Fundamental Design Choices

We focus here on three fundamental choices in the design of ad hoc networks [10]: the network architecture, the routing protocol and the medium access control.

4.3.2.1 Flat vs. Hierarchical Architecture

The architecture of ad hoc networks can be classified into *hierarchical* and *flat* architecture [10]. In a hierarchical architecture, the network nodes are dynamically partitioned into groups called clusters. Thus, the details of the network topology are concealed by aggregating nodes into clusters and clusters into superclusters and so on [11]. The membership in each cluster changes over time in response to node mobility and is determined by the criteria specified in the clustering algorithm. Within each cluster, one node is chosen to perform the function of a cluster head. [12]. Routing traffic between two nodes that are in two different clusters is normally done through the cluster heads of the source and destination clusters. A dynamic cluster head selection algorithm is used to elect a node as the cluster head. However, frequent change in cluster membership and consequent reselection of cluster head adversely affects routing protocol performance.

In contrast, in a flat architecture, there are no clusters and the neighbouring nodes can communicate directly. It has been argued that the routing in flat architecture is more optimal (close-by nodes do not have to communicate through the hierarchy) and the network tends to better balance the load among multiple paths, thus reducing the traffic bottlenecks that occur at the cluster nodes in the hierarchical approach [10].

The main advantage of the hierarchical ad-hoc network is the ease of the mobility management process. In order to limit far-reaching impact to topology dynamics, complete routing information is maintained only for intra-cluster routing. Inter-cluster routing is achieved by hiding the topology details within a cluster from external nodes and using hierarchical aggregation, reactive routing or a combination of both techniques. Cluster heads can act as databases that contain the "location" of the nodes in their own clusters. To determine the existence and the "location" of a mobile node, a query is broadcasted to all the cluster heads. The cluster, under which the node resides, responds to the query originator. Mobility management scheme needs to be implemented in the flat networks by appropriate routing algorithms, although it would increase the overhead due to control message propagation throughout the network [10].

4.3.2.2 Proactive vs. Reactive Routing

The existing routing protocol can be classified either as proactive or as reactive. In proactive protocols, the routing information within the network is always known beforehand through continuous route updates. The distance vector and link state protocols are examples of proactive scheme. Examples of proactive routing methods in ad hoc network environment are given in [13]. However, these methods require knowing the topology of the entire network and this information needs to be propagated through the network. As the network size increases and as the nodal mobility increases, smaller and smaller fraction of this total amount of control traffic will be even used. This is so, since as the nodes become more mobile, the lifetime of a link decreases. Thus, the period in which the routing information remains valid decreases as well. In fact, it is easy to show that for any given network capacity, there exists a network size and nodal mobility for which all the network capacity will be wasted on control traffic only [10]. Thus, in a highly dynamic environment, these schemes are less efficient. However, the advantage of the proactive schemes is that, once a route is needed, it is immediately available from the route table.

Reactive protocols, on the other hand, invoke a route discovery procedure on demand only. Thus, when a route is needed, some sort of flooding-based global search procedure is employed. The family of classical flooding algorithms belongs to this group. Examples of reactive protocols in the context of ad hoc networks are given in [13]. In these protocols, because route information may not be available at the time a route request is received, the delay to determine a route can be quite significant. Furthermore, the global search procedure of the reactive protocols generates significant control traffic.

Because of this long delay and excessive control traffic, pure reactive routing protocols may not be applicable to real-time communication. However, pure proactive schemes are likewise not appropriate for the ad-hoc network environment, as they continuously use a large portion of the network capacity to keep the routing information current. Thus, designing a proper routing scheme for ad hoc networks is a challenging task.

4.3.3.3 Medium Access Protocol

The medium in a wireless network is, by nature, a shared resource where a sender normally uses omni-directional broadcast mode to transmit a message for its intended destination. As a result, other users who are within the transmission range of the sender will also have to "listen" to its message even though they are not the intended receivers of this message. In this context, it is important to ensure a collision-free message communication environment even when multiple senders want to communicate with multiple receivers using the same-shared medium. Imagine a situation (Figure 4.2) with seven nodes (I, E, S, D, H, J and N) where a sender E is trying to send a message to a receiver I and another sender H is trying to send a message to another receiver J simultaneously. Let us also assume that I is within the transmission range of E only and J is within the transmission range of H only. In other words, I can only listen to E and not to H. Similarly J can only listen to H and not to E. This is a conflict-free communication environment where both communications can progress simultaneously without interfering with each other. However, this scenario is rare in a dynamic environment of ad hoc network Let us further assume that while E is talking to I, another node S wants to send a message to N. The node N is in the listening range of both E and S. So, there will be collision at receiver N and N will not be able to receive any message from S.

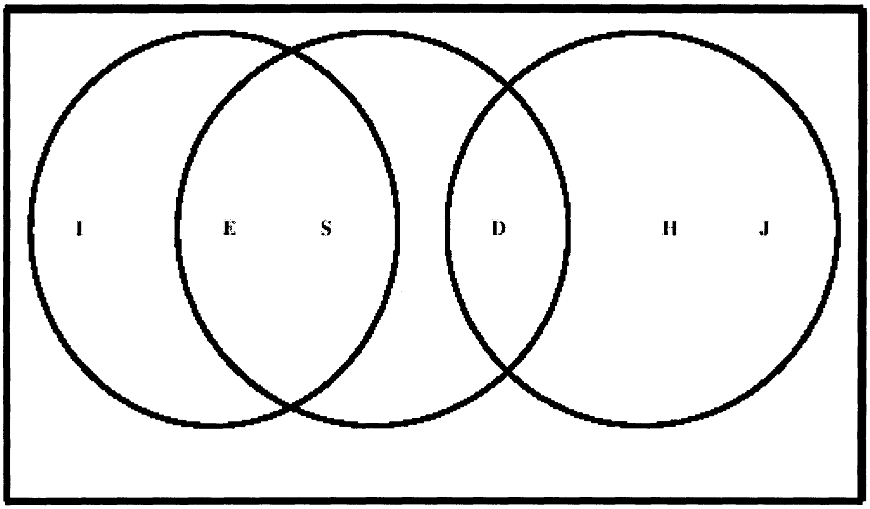


Figure 4.2 Hidden Terminal and Exposed Terminal problem

One way to solve the problem is to "sense" the medium before transmitting. So, S will first "sense" the medium to find out the existence of any on-going communication. Since E is already transmitting data and S is within the transmission range of E, S can "sense" that the medium is busy. So, S will defer its desire to transmit message towards N. However, this will give rise to what is known as Exposed Terminal Problem. Assume that S is transmitting to D. Since E senses an ongoing data transmission (i.e. E is "exposed" to the transmission by S), E remains silent. But E does not know that D is out of its reach. In fact, E could have transmitted to node I because these transmissions would not cause any collision either at D or at I.

A more serious problem is known as "Hidden Terminal Problem". Assume that node S is sending data to node D. A terminal H is "hidden" when it is far away from the data source S but is close to the destination D. Without the ability to detect the ongoing data transmission, H will cause a collision at D if H starts transmitting to J. Medium access control in this context implements mechanisms to prevent the collision at D by any hidden terminal (such as H).

The protocols based on RTS/CTS handshaking (Request-to-send/ Clear-to-send) can reduce the packet loss due to hidden terminals as follows:

Let us refer to Figure 4.2. Before sending the data packets, S sends RTS with proposed duration of data transmission to inform its neighbours about its willingness to start a communication with D. So, all the neighbours of S will become idle (neither transmit nor receive) during this period. If the intended destination D hears the RTS, D replies with CTS to inform its neighbours about its willingness to receive data from S. The neighbours of D that receives *only* CTS cannot transmit (to avoid collision with D's reception), but they can receive from other nodes outside the RTS/CTS boundaries. In some protocols, another packet called *data-sending* (DS) packet is issued by S after it receives the CTS packet in order to ensure its neighbours that a successful reservation has been accomplished. This avoids unwanted waiting of nodes receiving only RTS under the condition of unsuccessful negotiation between S and D. After data reception by D is over successfully, it issues an ACK (acknowledgement) to S. The acknowledgement (ACK) packet at link level speeds up packet retransmission that is faster than relying on the slow recovery at the transport layer.

Any other nodes overhearing the RTS must be close to node S and therefore should remain silent for a time period long enough so that node S can receive the returning CTS without any collision. Any other nodes overhearing the CTS must be close to node D and therefore should refrain from transmission for a time period that is long enough for the transmission of the proposed data packet so that node D can receive the returning data packet without any conflict. A hidden terminal (e.g. node H), which is in the range of node D but out of the range of node S, will hear the CTS but not the RTS. It, therefore, remains silent during the data transmission from node S to node D.

Researchers are still working to address several performance concerns of MAC protocols proposed in the context of ad hoc networks [14]. Use of directional antenna to improve medium utilization is an active area of research [15]. One of the important issues is to ensure fairness in medium access. In a multi-hop configuration using CSMA/CA based MAC protocols with exponential back-off mechanism, all the nodes may not be able to access the shared medium equally well all the time. This results in severe performance degradation. The performance degrades further, if we assume asymmetric links. Note that all the above protocols assume the presence of symmetric links. This is valid for a network in which all nodes transmit at the same power level. However, an ad hoc network may comprise of devices that have different transmit power capabilities. In any event, it will be critical to ensure that the MAC protocol in use does not unduly favour devices that can transmit at higher power levels [16]. Researches are also focusing on power controlled MAC protocols that would improve channel utilization to a large extent [17-18]. The basic idea behind conventional CSMA/CA MAC protocol is to reserve the transmission and reception areas of both source and destination. The goal of power-controlled MAC is that, a pair of communicating nodes adjusts their power-level to acquire the minimum area of the floor that is needed for it to successfully complete a data transmission [18].

4.4 FIXED-ACCESS WIRELESS SYSTEMS IN METROPOLITAN AREA (WMAN)

WMANs have been using fixed-access wireless technologies such as point-to-point microwave and optical systems. They are expensive and time-consuming to install, but delivers high bandwidth and reliability. Line of sight is required for these systems, and their range is limited only by the curvature of the Earth. More recently, lower-cost radio-based systems using unlicensed spectrum in the 2.4- and 5-GHz bands have become increasingly popular. They do not require FCC license and thus have become a popular solution for interconnecting two sites; for example, remote cellular-telephone sites back to central points of presence in metropolitan areas. Performance ranges from 1.5 Mbps to more than 50 Mbps. While there are risks associated with the use of unlicensed spectrum, well-designed systems are quite tolerant of interference.

Although DSL and cable modems are widely acknowledged as the leading metropolitan-area broadband-access technologies, broadband wireless is emerging as a viable alternative, especially where DSL and cable services are not readily available. The FCC recently implemented changes that give service providers greater flexibility to provide MMDS (Multichannel Multipoint Distribution Service), a multimegabit wireless service operating in the 2.5-GHz band. The Wireless DSL Consortium was also formed with the goal of establishing open standards for MMDS access. Compared with earlier-generation LMDS (Local Multipoint Distribution Service) technologies, MMDS has greater range -- up to 35 miles -- and greater throughput [19].

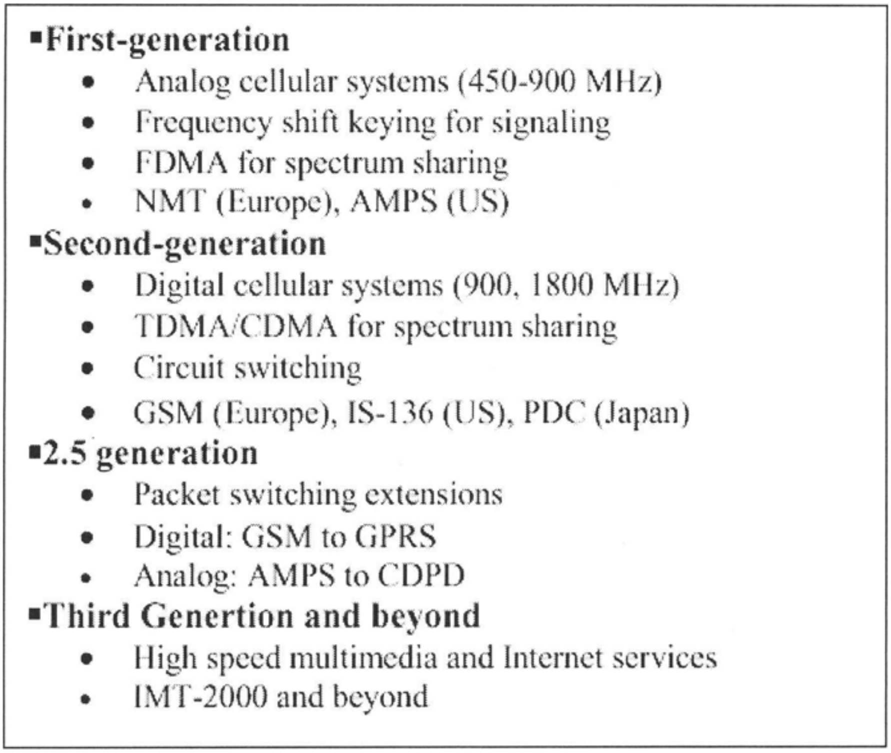
Another technology in this category is Wireless Local Loop (WLL). A Local Loop connects each telephone subscriber's line to the telephone company's central office. Wireless technology in local loop applications is essentially providing fixed wireless access to the telephone network by the subscribers. Wireless connectivity to subscribers today is provided by mobile communication systems as well as wireless in local loop systems. These two appear to be similar and are often confused with each other. However, the requirements for the two systems are significantly different [20]. Mobile Telephone systems are primarily meant to provide telephony for people on the move. The key here is universal coverage. So, location tracking and mobility management is a key feature in this system, as will be discussed in the next section. Wireless in Local Loop (WiLL), on the other hand, is meant to serve subscribers at homes or offices. It is a fixed wireless access to the telephone exchange that supports limited mobility within the coverage area of the exchange. So, the telephone service provided must be as good as wired phone. It must support fax and modem communications as good as wired phone. Further, ability to support a large number of subscribers in an urban area with a limited frequency spectrum is required.

4.5 WIRELESS WAN

The major goal of mobile wireless access is to allow a user to have access to the capabilities of the global network at any time without regard to location or mobility. The popularity of the Internet may be a defining feature of the interest in wireless WANs, which can allow the Internet access from anytime, anywhere. At the same time, a mobile user desires to communicate with another user or group anytime, anywhere, with voice/video/data. However, this goal is still far away because of the lack of standards, speed, and bandwidth.

Since the inception of cellular telephones in early 1980s, it has been evolving from a costly service with limited availability toward an affordable but more versatile alternative to wired telephony [21]. Observing the trends, it can be predicted that the traffic over next generation, high speed wireless networks will be dominated by personal multimedia applications such as fairly high speed data, video and multi media traffic. The technology needed to tackle the challenges is known as third generation systems [22]. From this viewpoint, early analog cell phones are labeled as first generation, and similar systems featuring digital radio technologies are labeled as second generation. Principal advantages of second generation systems over their analog predecessors are greater capacity and less frequent need for battery charging. In other words, they accommodate more users in a given piece of spectrum and they consume less power. However, second generation networks retain the circuit switching legacy of analog networks. They were all designed to carry voice traffic, which has little tolerance for delay. Data services are more tolerant of network latencies. The evolution is shown in Figure 4.3.

Today's second-generation wireless infrastructure typically supports a maximum transmission speed of 14.4 Kbps that is sufficient only for the most rudimentary text-oriented applications other than voice traffic. It is a challenging task to overlay high-speed data services on top of an existing voice infrastructure. Thus, achieving the long-term vision of interactive voice/video/data on mobile devices will require significant technical breakthroughs. While widespread deployment of 3G networks is yet to be seen, interim solutions like two-way messaging, using existing low-bandwidth infrastructure, is gaining in popularity as a mechanism for exchanging small amounts of digital content with mobile users over a wide area.



▪First-generation

- Analog cellular systems (450-900 MHz)
- Frequency shift keying for signaling
- FDMA for spectrum sharing
- NMT (Europe), AMPS (US)

▪Second-generation

- Digital cellular systems (900, 1800 MHz)
- TDMA/CDMA for spectrum sharing
- Circuit switching
- GSM (Europe), IS-136 (US), PDC (Japan)

▪2.5 generation

- Packet switching extensions
- Digital: GSM to GPRS
- Analog: AMPS to CDPD

▪Third Genertion and beyond

- High speed multimedia and Internet services
- IMT-2000 and beyond

Figure 4.3 Evolution of mobile wireless cellular system

However, third-generation wireless and beyond (3Gwireless and 4Gmobile) have continued to be the research focus over the last few years. 3Gwireless will use new network architecture (e.g., an all-IP network) to deliver broadband services in a more generic configuration to mobile customers and supports multidimensional services and emerging interactive multimedia communications. Large bandwidth, guaranteed quality of service, and ease of deployment coupled with recent great advancements in semiconductor technologies for wireless applications make 3Gwireless a very attractive solution for broadband service delivery [22].

4.5.1 Basic Cellular Architecture

The basic architecture of cellular networks is shown in Figure 4.4. Entire service-space is divided into a number of cells, where each cell is served by a base station (BS). A base station is responsible to communicate with mobile hosts (end-users) within its cell. When a mobile host changes its cells while communicating, hand-off occurs, and the mobile host starts communicating via a new base station and the mobile is able to continue communication seamlessly throughout the network. Each BS is connected to a mobile switching center (MSC) through fixed links. Each MSC is connected to other MSCs and PSTN (public switched telephone network).

Each MSC handles two major tasks:

- switching of mobile user from one base station to another and
- locating the current cell of a mobile user.

The MSCs communicate with location registration databases such as the home location register (HLR) and the visitor location register (VLR) to provide roaming management. Home Location Register (HLR) at each MSC is a database recording the current location of each mobile that belongs to the MSC. And, Visitor Location Register (VLR) at each MSC is a database recording the cell of "visiting" mobiles.

The distinguishing feature of cellular systems compared to previous mobile radio systems is the use of many base stations with relatively small coverage radii of the order of 10 km or less vs. 50 to 100 km for earlier mobile systems. Frequency reuse among non-adjacent cells allows a much higher subscriber density per MHz of spectrum than previous systems. System capacity can be further increased by reducing the cell size (the coverage area of a single base station).

In order to support higher subscriber densities, cell size can be reduced further than previous systems, down to radii as small as 0.5 km. This system also allows the user to use small, battery-powered portable handsets with lower transmit power than the large vehicular mobile units used in earlier systems. In cellular systems, continuous coverage is achieved by executing a "handoff" (the seamless transfer of the call from one base station to another) as the mobile unit crosses cell "boundaries." This requires the mobile to change frequencies under control of the cellular network.

There are several techniques for handoff because it may not always be possible to get a frequency in the new cell for a handoff call. For example, if all the frequencies in the next cell is currently under use, the handoff call has to be dropped, which is certainly not desirable for the concerned user. It also degrades the QoS for the network. So it is preferable to reserve a set of frequencies in every cell for handoff calls so that an onging call is not terminated. This, in turn, leads to many call admission policies.

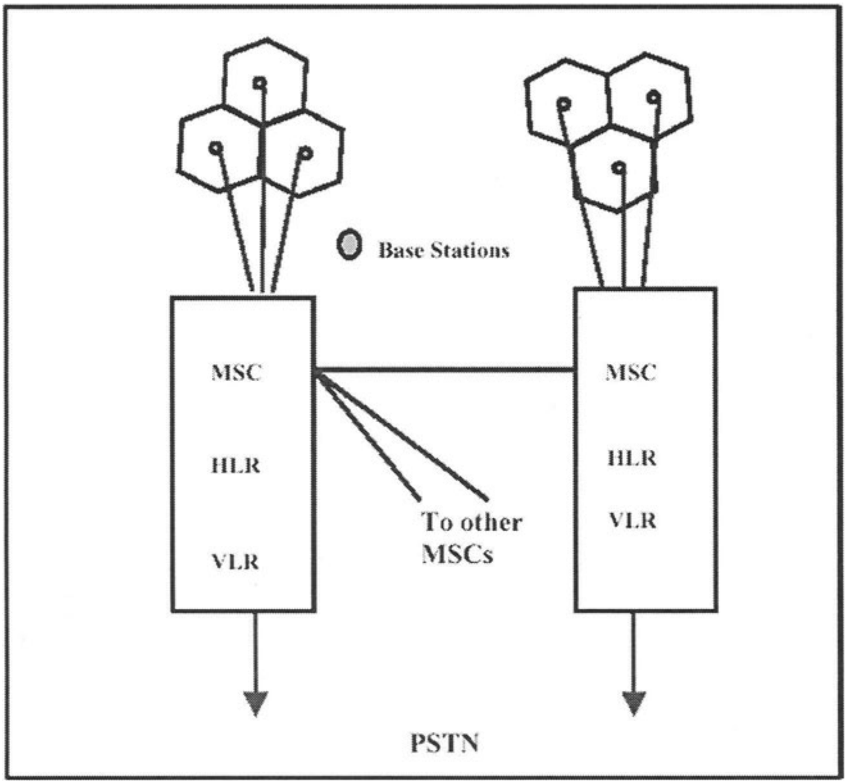


Figure 4.4 The Architecture of Basic Cellular Network

4.5.2 Location Management

Mobility can be categorized into two areas: Radio mobility, which mainly consists of the handover process and Network mobility, which mainly consists of location management (location updating and paging) [1].

A network must retain information about the locations of endpoints in the network, in order to route traffic to the correct destinations. Location tracking (also referred to as mobility tracking or mobility management) is the set of mechanisms by which location information is updated in response to endpoint mobility. In location tracking, it is important to differentiate between the identifier of an endpoint (i.e., what the endpoint is called) and its address (i.e., where the endpoint is located). Mechanisms for location tracking provide a time varying mapping between the identifier and the address of each endpoint. Most location tracking mechanisms may be perceived as updating and querying a distributed database (the location database) of endpoint identifier-to-address mappings. In this context, location tracking has two components: (1) determining when and how a change in a location database entry should be initiated; and (2) organizing and maintaining the location database. In cellular networks, endpoint mobility within a cell is transparent to the network, and hence location tracking is only required when an endpoint moves from one cell to another. Location tracking typically consists of two operations: (1) updating (or registration), the process by which a mobile endpoint initiates a change in the location database according to its new location; and (2) finding (or paging), the process by which the network initiates a query for an endpoint's location (which may also result in an update to the location database). Most location tracking techniques use a combination of updating and finding in an effort to select the best tradeoff between update overhead and delay incurred in finding. Specifically, updates are not usually sent every time an endpoint enters a new cell, but rather are sent according to a pre-defined strategy such that the finding operation can be restricted to a specific area. There is also a tradeoff, analyzed formally between the update and paging costs. The location management methods are most adapted and widely used in current cellular networks e.g. GSM, IS-54, IS-95, etc. The location management methods are broadly classified into two groups. The first group includes all methods based on algorithms and network architecture, mainly on the processing capabilities of the system. The second group contains the methods based on learning processes, which require the collection of statistics on subscribers' mobility behavior, for instance. This type of method emphasizes the information capabilities of the network.

4.5.3 Radio Resource Management

The problem of radio resource management is one important issue for good network performance. The radio resource management problem depends on the three key allocation decisions that are concerned with waveforms (channels), access ports (or base stations) and with the transmitter powers. Both channel derivation and allocation methods will influence the performance. The use of time division multiple access (TDMA) and code division multiple access (CDMA) are alternatives to FDMA used in the first generation systems. With TDMA, the usage of each radio channel is partitioned into multiple timeslots, and each user is assigned a specific frequency/timeslot combination. Thus, only a single mobile in a given cell is using a given frequency at any particular time. With CDMA, multiple mobiles in a given cell use the channel simultaneously, and the signals are distinguished by spreading them with different codes. The channel allocation is an essential feature in cellular networks and impacts the network performance. These different access technologies are used in different standards in 2G/3G systems.

4.6 DISCUSSION

A future wireless telecommunication system should focus on the integration of multiple wireless access technologies (terrestrial and satellite) towards a core network infrastructure, which could be based on IP networking technology. Driven by the need for wireless Internet access, the fourth-generation wireless system will be a converged platform for broadband mobile and broadband access. The system's vision of broadband wireless mobile (e.g., 4Gmobile) is to: provide a technological response to accelerated growth in the demand for broadband wireless connectivity; ensure seamless services provisioning across a multitude of wireless systems and networks, from private to public, from indoor to wide area; provide optimum delivery of the user's wanted service via the most appropriate network available; cope with the expected growth in Internet-based communications and opening new spectrum frontiers and creating new market opportunities.

REFERENCES

[1] S. Ramanathan and M. Steenstrup, "A survey of routing techniques for mobile communications networks," ACM/Baltzer Mobile Networks and Applications, Vol. 1, No. 2, pp. 89-103.

[2] D. Johnson, "Routing in Ad Hoc Networks of Mobile Hosts," in Proc.IEEE Workshop on Mobile Comp. Systems and Appls., Dec. 1994.

[3] Joseph m. Kahn, and John r. Barry, Wireless Infrared Communications", Proceedings of the IEEE, Vol. 85, no. 2, February 1997.

[4] Walter Hirt, Martin Hassner and Nyles Heise, " IrDA-VFIr (16 Mb/s): Modulation Code and System Design" IEEE Personal Communications, Vol. 1, No. 1, February 2001

[5] Peter Barker, Anthony Boucouvalas, "A simulation model of the Advanced Infrared (AIr) MAC protocol using OPNET", Second International Symposium on Communications Systems Networks and Digital Signal Processing, (CSNDSP 2000), 18-20 July 2000, Bournemouth University, UK, pp 153 -156

[6] http://www.zurich.ibm.com/cs/wireless/ircommunication.html

[7] Theodoros Salonidis, Pravin Bhagwat,Leandros Tassiulas, Richard LaMaire, "Proximity Awareness and Ad Hoc Network Establishment in Bluetooth, Technical Research Report CSHCN T.R. 2001-2 http://www.isr.umd.edu/TechReports/CSHCN/2001/CSHCN_TR_2001-1/ CSHCN_TR_2001-1.pdf.

[8] S. Corson, J. Macker and S. Batsell, "Architectural Considerations for Mobile Mesh Networking", Internet Draft RFC Version 2, May 1996.

[9] E. M. Royer and C-K Toh, “A Review of Current Routing Protocols for Ad hoc Wireless Networks”, IEEE Personal Communication, April 1999, pp. 46-55.

[10] Z.J. Haas and S. Tabrizi, "On Some Challenges and Design Choices in Ad-Hoc Communications,"IEEE MILCOM'98, Bedford, MA, October 18-21, 1998

[11] G. S. Lauer, "Packet-Radio Routing," M. E. Steenstrup, editors, Routing in Communications Networks, Prentice-Hall, 1995, pp.375-379.

[12] M. Gerla and J. T. Tsai, "Multicluster, Mobile, Multimedia Radio Network," ACM Wireless Networks, Vol.1, No.3, 1995, pp.255-265.

[13] S.-J. Lee, M. Gerla, and C.-K. Toh, ``A Simulation Study of Table-Driven and On-Demand Routing Protocols for Mobile Ad-Hoc Networks," IEEE Network, vol. 13, no. 4, Jul. 1999, pp. 48-54.

[14] Does the IEEE 802.11 MAC Protocol work well in Multihop Aireless Ad Hoc Networks? S. Xu and T. Saadawi, IEEE Communication Magazine, June 2001, pp130-137.

[15] S. Bandyopadhyay, K. Hasuike, S. Horisawa, S. Tawara, “An Adaptive MAC Protocol for Wireless Ad Hoc Community Network (WACNet) Using Electronically Steerable Passive Array Radiator Antenna”, GLOBECOM 2001, November, San Antonio, Texas, USA

[16] Poojary, N., Krishnamurthy, S.V. and Dao, S, Medium Access Control in a Network of Ad Hoc Nodes with Heterogeneous Transmit Power Capabilities, Proceedings of ICC 2001, Helisinki.

[17] Shih-Lin Wu and Yu-Chee Tseng, “Intelligent Medium Access for Mobile Ad Hoc Networks with Busy Tones and Power Control” JSAC vol 18 no 9 Sept 2000.

[18] Jeffrey P. Monks, Vaduvur Bharghavan, and Wen-mei Hwu, "A Power Controlled Multiple Access Protocol for Wireless Packet Networks," IEEE INFOCOM 2001, Anchorage, Alaska, April, 2001.

[19] Bolcskel, H.; Paulraj, A.J.; Hari, K.V.S.; Nabar, R.U.; Lu, Willie W., “Fixed Broadband Wireless Access : State of the Art, Challenges and Future Directions, IEEE Communications Magazine , Volume: 39 Issue:1 January 2001

[20] Ashok Jhunjhunwala, Devendra Jalihal, K.GiridharWireless in Local Loop — Some Fundamentals, Technical Report, Telecommunications and Networks (TeNeT) Group, Dept. of Electrical Engineering, IIT Madras, Chennai 600 036, INDIA, Dec 2000.

[21] Jay E. Padgett, Christoph G. Günther, and Takeshi Hattori, “Overview of Wireless Personal Communications”, IEEE Communications Magazine • January 1995.

Chapter 5

Interface Technology

From users' point of view, a PervComp environment is a space that contains myriad devices that work together to provide users pervasive access to information and services. These devices may be stationary, as with refrigerators or acoustic speakers or ceiling lights, or they may be mobile, as with tracking sensors, laptop computers or mobile telephones. While the traditional notion of a PC is certainly a part of this vision, a broader goal, as outlined in Chapter 1, is to allow typical PC-focused activities to move off of a fixed desktop and blend into the environment as a whole. Additional to these user-centric I/O devices, there will also be devices dedicated to providing communication and computational capacity to the system; but they will be transparent to the users. So the goal of the user-interface layer in PervComp is the development of a system that aggregates diverse devices into a *coherent* user experience. Needless to say, this requires research effort on a variety of fronts, including interoperability, interworking, middleware, smart adapters, world perception, intelligent networking, and service description. However, we restrict ourselves to those components, which are relevant to PervNet, and discuss about them in this chapter under the heading "Interface Technology" because they act as interface between the core of PervNet and the set of user applications to facilitate PervComp.

5.1 USER INTERFACE

As discussed in Chapter 2, PervNet is targeted to support a distributed system explicitly designed to operate in environments, which involve billions of machines simultaneously, plus many end-users. Network connections between machines in the system have very diverse characteristics in terms of latency, bandwidth, reliability, etc. It spans over many different administrative domains. It is an ad-hoc wide-area distributed system much similar to the World-Wide Web but in a bigger scale. On the other hand, PervComp, as visualized in Chapter 1, incorporates a variety of sensing techniques, software components for reasoning, and controllable devices, such as lights, computer equipment, and audio/visual hardware. Each of these pieces is encapsulated in a unique service, which encourages the isolation of hardware device control, internal network, and user interface presentation. Multiple types of networks at one end and pervasive applications at the other end motivate the need for the separation of network control from applications through appropriate *user interface presentation*. Rather than tightly coupling PervNet to pervasive applications, it should be possible to flexibly change the interaction mechanism without requiring modification of either the underlying PervNet or the pervasive applications. Middlewares usually enable this kind of decomposition by providing abstract descriptions of the service capabilities, which allow each service to expose a set of attributes or commands so that other services may interact with it automatically. It is true that, in order to support pervasive computing, many of the traditional activities of an operating system must be supported across a distributed heterogeneous set of networked devices. As the number of available networked devices for a given user interaction increases, the complexity of identifying and selecting the appropriate devices for that interaction increases greatly. Furthermore, for the user to be able to specify which devices he/she wishes to use for a given task, a mapping between network and physical identity is exceptionally helpful.

As conveyed above, given a PervNet (i.e., a collection of networked devices), the need arises for a mechanism that supports inter-machine communication. By utilizing a middleware package, the effort required to build individual components that can communicate in this distributed environment is reduced. Several packages are currently available for this task, such as Microsoft DCOM [1], [2] Java [3], Jini [4], and OMG's CORBA [5]. Furthermore, legacy applications can be integrated by communicating through standard networking protocols, such as HTTP or SOAP [6], and by exchanging data in standard formats, such as XML.

5.2 MIDDLEWARES

We have seen in Chapter 1 that middleware is one of the four major PervComp components. Perhaps, it is the most grey and hence least attended area of PervComp thus far. However, without it, PervNet will not be able to deliver the desired effect up to the user level. In a sense, we have encountered a subset of the middleware-related problems earlier in distributed computing and mobile computing (see Sections 1.2 and 1.3). However, the necessity of catering for the constant change in number and type of pervasive devices of interest to a user, as well as their sheer quantity, dictates new approaches to construction of middleware systems based on more flexible models. The middleware challenges offered by the previous generation of networks are being answered by technologies like Plug and Play, XML, Java and Jini; but the grand challenges of PervNet remain unanswered simply because the current software and network architectures and their associated programming paradigms will not scale to this new world of PervComp.

5.2.1 Models

The role of middleware is to ease the task of designing, programming and managing distributed (both mobile and static) applications by providing a simple, consistent and integrated distributed programming environment. Essentially, middleware is a *distributed software layer*, or 'platform' which abstracts over the complexity and heterogeneity of the underlying distributed environment with its multitude of network technologies, machine architectures, operating systems and programming languages. Different middleware platforms support different programming models. There are three popular models (paradigms) based on *object*, *event* and *message* in place now-a-days. In object-based middleware, applications are structured into (potentially distributed) objects that interact via location transparent method invocation. Message-oriented middleware is biased toward applications in which messages need to be persistently stored and queued. Event-based and message-oriented middlewares mainly employ 'single shot' communications rather than the request-reply style communication found in object-based middleware. Workflow and messaging applications are good examples of message-oriented middleware. Among the three models, object-based middleware is perhaps the most popular model exemplified by the CORBA [5] and DCOM [1]. Both of these platforms offer 1) an interface definition language (IDL) which is used to abstract over the fact that objects can be implemented in any suitable programming language, 2) an object request broker which is responsible for transparently directing method invocations to the appropriate target object, and 3) a set of services (e.g., naming, time, transactions, replication etc.) which further enhance the distributed programming environment. However, an event-based middleware is particularly suited to the construction of non-centralized distributed applications that must monitor and react to changes in their environment. Examples are process control, Internet news channels and stock tracking.

Since event-based middleware has potentially better scaling properties than object based middleware, for PervComp applications it may be the better option.

5.2.2 Semantics

Current middleware environments, such as DCOM [1], Java [3], and CORBA [5], are built on synchronous semantics and, hence, suffer from several failings. First, they force programmers to employ a multithreaded programming model, if they wish to avoid the latencies inherent in synchronous communications. For example, a single-threaded program that needs to interact with multiple peers would have to serialize its interactions with them rather than engaging in multiple interactions simultaneously. A single-threaded program will also be unable to do other useful work while waiting for a reply from a remote server. Worse yet, should the server fail or become unreachable, the program or device will be locked-up until a delivery time-out is reached.

A second failing of synchronous communication techniques is that pipelining of messages between two endpoints is very inefficient, even in a multi-threaded environment. If both the sending and receiving programs are multi-threaded, then by having each program fork multiple threads that communicate in parallel, pipelining can be approximated. However, for messages to have a well-defined arrival order, both the sending and the receiving programs must individually implement message serialization code. Furthermore, it would still not be possible to have only a single reply message for an entire batch of pipelined messages.

5.2.3 Data and Functionality

Several distributed systems, targeted at a global computing environment, have explored the use of objects as the unifying abstraction for both data and functionality. However, many are skeptical about this use of objects for distributed computing for two reasons. First, objects as an encapsulation mechanism are based on two assumptions: (1) Implementation and data layout change more frequently than an object's interface, and (2) it is indeed possible to design interfaces that accommodate different implementations and hold up as a system evolves. However, these assumptions do not hold for a global distributed computing environment.

Increasingly, common data formats, such as HTML or PNG, are specified by industry groups or standard bodies, notably the World Wide Web Consortium, and evolve at a relatively slow pace. In contrast, application vendors compete on functionality, leading to considerable differences in application interfaces and implementations and a much faster pace of innovation. Second, it is preferable to store and communicate data instead of objects, as it is generally easier to access passive data rather than active objects. In particular, safe access to active objects in a distributed system raises important issues, notably system security and resource control, which are less difficult to address when accessing passive data. This is clearly reflected in today's Internet; for example, access to regular HTML or PDF documents works well, while active content results in an ever-continuing string of security breaches. Based on the above two realizations, it is generally felt that data and functionality should be kept separate rather than being encapsulated within objects.

At the same time, data and functionality depend on each other, especially when considering data storage and mobile code. On one hand, data management systems already rely on mobile code for their services. For example, Bayou propagates updates as procedures and not simply as data. The Oracle8*i* database not only supports SQL stored procedures, but also includes a fully featured Java virtual machine. On the other hand, mobile code systems have seen limited success in the absence of a standard data model and the corresponding data management solutions. For example, while many projects have explored mobile agents, they have not been widely adopted, in part because they lack storage management. Java, which was originally marketed as a mobile code platform for the Internet, has been most successful in the enterprise, where access to databases is universal. The result is a considerable tension between integrating data and functionality too tightly (say, in the form of objects) and not integrating them tightly enough. One possible way to resolve this tension is to keep data and functionality separate and by introducing a new, higher-level abstraction to group the two. For instance, data may be represented by tuples, which essentially are records with named and optionally typed fields, while functionality is provided by components, which implement units of functionality. To summarize, data and functionality need to be supported equally well in PervComp, yet also need to be kept separate.

5.2.4 Application Programming Interface (API)

Another desirable feature for a PervWare is a single application programming interface (API) and a single binary distribution format, including a single instruction set, that can be implemented across the range of devices in a pervasive computing environment. A single, common API makes it possible to develop applications once, and a single, common binary format enables the automatic distribution and installation of applications. It is important to note that Java does not provide this common platform. While the Java virtual machine is attractive as a virtual execution platform (and used for this purpose by *one.world* project), Java as an application platform does not meet the needs of the pervasive computing space. In particular, Java's platform libraries are rather large, loosely integrated, and often targeted at conventional computers. Furthermore, Java, by itself, fails to separate data and functionality and does not encourage programming for change.

5.3 INTELLIGENT ENVIRONMENT

Intelligent environment is another way to solve the interfacing problem in PervComp. It serves as a unifying abstraction for user interface. In a sense, it is a container for data, functionality, middleware components, and other environments, providing a combination of the roles served by legacy operating systems and user interfaces in an enhanced scale. For example, since an intelligent environment must support a changing collection of devices (and therefore services), it is necessary to handle service discovery. Moreover, intelligent environments must determine the newly found service's capabilities in order to make it possible to group data and functionality when necessary. This allows data and functionality to evolve separately, and applications are allowed to store and exchange just data.

It is a well-known fact that the concept of abstracting and describing services arises naturally when developing a system that involves automatic interaction between program components or exposure of device attributes. Several commercial systems, such as Universal Plug and Play [7], provide for device descriptions. However, they fail to differentiate between the interface presentation and service description. Some systems have proposed separating device control from decision logic but did not allow for configuration changes. Some others have encoded context information into the XML service descriptions, but did not separate the service semantics from the service description. Most of the intelligent environment systems have not dealt with dynamic location-dependent services and automatically generated user interfaces. However, a service description schema may be designed to support queries about available services and their resources.

A large portion of any intelligent environment will comprise middlewares for handling context awareness or for sensing user perceptions. For instance, the person tracking software [8] has been used in Microsoft's Easyliving project [9]. Therefore, it is desirable to have commands, which are associated with human-readable tags. While not a complete solution, this may be a first step toward the automatic generation of user interfaces for different modalities.

5.4 SMART ADAPTERS

The existence of smart spaces in PervComp suggests that some of the environments encountered by a user may be capable of adapting itself. PervNet experiences dynamic configuration changes leading to a significant mismatch between the supply and demand of a service or a resource. For example, the resource may be wireless network bandwidth, energy, computing cycles, memory, and so on; the requested service may be premium quality message delivery, strong security encryption, and so on. Hence, adaptation is necessary to smoothen out these jitters in services/resources while moving from PervNet to PervComp. Smart adapters are responsible for doing this middleware job. For example, if current resources support pointing via trackball, mouse or visual gesture and, for each of these methods, there is a service that generates a pointing output, a smart web browser can be driven by any of those services, dependent upon user preference, context, or other selection mechanism.

Another example is the smart adaptation of the processes, which describe the target for a message. In PervComp, it will be common occurrence that users frequently transition between laptops, desktops, and home machines. This implies that components that are linked to a user may need to transition between varieties of machines in order to retain network proximity. Currently, DCOM [1] and Java [3] require machine names as part of the address for the message. CORBA [5] provides for an object reference, but does not allow that reference to be updated dynamically. This results in delivery problems when the target is moved to another machine.

Beyond the problems of delivering messages to processes is the issue of message encoding. Most of the systems rely on fully decorated method names for communication endpoint bindings. This forces the clients to be updated in lock step with the server. This means changes must be done *en masse* rather than incrementally and that offline devices, like an out-of-reach laptop, must be updated upon joining the network. Mobile devices also often change both physical location and network connectivity as they move with the user. These devices are added and removed from the collection of available hardware in a particular environment. Finally, for load balancing, many services are hardware independent and may be stopped on one machine and restarted on a different machine. In each of these situations, smart adaptation is essential.

There are several strategies for adaptation. An adapter can guide applications in changing their behavior so that they use less of a scarce resource. This change usually reduces the user-perceived quality, or fidelity, of an application. Alternatively, the adapter can ask the PervNet to guarantee a certain QoS. If the PervNet reacts on this request, it is likely (but not certain) that resource supply will become adequate to meet demand. In another approach, adapter can suggest a corrective action to the PervNet. The existence of smart adapters suggests that some of the environments encountered by a user may be capable of accepting resource reservations. At the same time, uneven conditioning of environments suggests that an adapter may not succeed always, particularly when the PervNet is uncooperative or resource-impoverished.

5.5 RELATED PROJECTS

In this section, we discuss some typical PervWare initiatives, being pursued at different parts of the world, under respective headings that specify their characteristics in short. This is not an exhaustive list. It only aims to give the readers a glimpse of what kind of research issues are important in this area and how much development has been achieved thus far.

5.5.1 Distributed File Systems

5.5.1.1 AFS

This project [16] began in 1983 in the context of Andrew, a joint project of CMU and IBM to develop a state-of-the-art computing facility for education and research at CMU. The project envisioned a dramatic increase in computing power made possible by the widespread deployment of powerful personal workstations. The objective of the project was to develop a mechanism that would enable the users of these workstations to collaborate and share data effectively. The project had decided to build a distributed file system for this purpose because it would provide the right balance between functionality and complexity for our usage environment. Their design has evolved over time, resulting in three distinct versions of the Andrew file system, called AFS-1, AFS-2, and AFS-3. In this article "Andrew file system" or "Andrew" will be used as a collective term referring to all three versions. As their (the project's) user community became more dependent on Andrew, the availability of data in it became more important. Today, a single failure in Andrew can seriously inconvenience many users for significant periods. To address this problem, they began the design of an experimental file system called Coda in 1987. Intended for the same computing environment as Andrew, Coda retains Andrew's scalability and security characteristics while providing much higher availability.

5.5.1.2 Coda

Many aspects of Coda [17] are inherited from the *Andrew file system* (AFS), a large-scale distributed file system. Coda is a file system for a large-scale distributed computing environment composed of Unix workstations. It provides resiliency to server and network failures through the use of two distinct but complementary mechanisms. One mechanism, *server replication,* involves storing copies of a file at multiple servers. The other mechanism, *disconnected operation,* is a mode of execution in which a caching site temporarily assumes the role of a replication site. Disconnected operation is particularly useful for supporting portable workstations. The design of Coda optimizes for availability and performance, but provides the highest degree of consistency attainable in the light of those objectives. Measurements from a prototype show that the performance cost of providing high availability in Coda is reasonable.

5.5.2 Distributed Components

The formation of a distributed system from a collection of individual components requires the ability for components to exchange syntactically well-formed messages. Several technologies exist that provide this fundamental functionality, as well as the ability to locate components dynamically based on syntactic requirements. The formation of a correct distributed system requires, in addition, that these interactions between components be semantically well formed.

5.5.2.1 Infospheres

The Caltech Infospheres Infrastructure (II) [18] is a distributed system framework that is implemented in Java. It provides a generic object model and a variety of messaging models: asynchronous, synchronous, and remote procedure calls. In June 1997, this research group released Infospheres 1, a preliminary version of the infrastructure for developing global distributed systems using Java and Internet technologies. In 1998, this project released a more flexible, robust Infospheres 2; although the implementation uses Java, XML, and Internet technologies, the ideas are applicable to distributed object systems based on other tools such as CORBA and DCOM.

This project has explored the four main attributes of the distributed systems: compositionality, scalability, dynamic reconfigurability, and high confidence. They have used temporal logic for reasoning about the correctness of distributed object systems and stochastic processes for reasoning about performance and reliability.

5.5.3 Global Computing

5.5.3.1 Legion (http://legion.virginia.edu/)

Legion, an object-based meta-systems software project at the University of Virginia, is designed for a wide-area virtual environment of the future. It is claimed as a worldwide virtual computer system (i.e., PervComp) of millions of hosts and trillions of objects tied together with high-speed links. Users working on their home machines see the illusion of a single pervasive computer, with access to all kinds of data and physical resources, such as digital libraries, physical simulations, cameras, linear accelerators, and video streams. Groups of users can construct shared virtual workspaces, to collaborate research and exchange information. This abstraction springs from Legion's transparent scheduling, data management, fault tolerance, site autonomy, and a wide range of security options.

As new requirements and new opportunities for PervComp emerge and future users make unforeseen demands on resources and software, the demands placed on the pervasive computer will evolve and grow. Legion is an open system, designed to encourage third party development of new or updated applications, run-time library implementations, and core components. Legion sits on top of the user's operating system, acting as a liaison between its own host(s) and whatever other resources are required. The user is not bogged down with time-consuming negotiations with outside systems and system administrators, because Legion's scheduling and security policies act on his/her behalf. Conversely, it can protect its own resources against other Legion users, so that administrators can choose appropriate policies for who uses which resources under what circumstances. To allow users to take advantage of a wide range of possible resources, Legion offers a user-controlled naming system called *context space*, so that users can easily create and use objects in far-flung systems. Users can also run applications written in multiple languages, because Legion supports interoperability between objects written in multiple languages.

5.5.3.2 Punch

PUNCH [19] is a platform for Internet computing that turns the World Wide Web into a distributed computing portal. Network-centric computing promises to revolutionize the way in which computing services are delivered to the end-user. Users can access and run programs via standard Web browsers. Applications can be installed as is in as little as thirty minutes. Machines, data, applications and other computing services can be located at different sites and managed by different entities. PUNCH provides a network operating system, logical user accounts, a virtual file system service that can access remote data on-demand, and an active yellow pages service. Together, these capabilities allow PUNCH to manage and broker resources among end users, application service providers, storage warehouses, and CPU farms. Delivering computing as a service requires that the underlying infrastructure be able to negotiate resources between institutional boundaries. PUNCH facilitates the negotiation by dynamically assembling systems of systems at run-time. PUNCH decouples the computing environment perceived by users from the underlying physical infrastructure, thus turning individual computing systems into interchangeable parts. This feature is key to PUNCH's ability to manage large numbers of users and resources that are spread across.

5.5.3.3 RaDaR

As commercial interest in the Internet grows, more and more companies are offering hosting services i.e. the service of hosting and providing access to objects belonging to third-party information providers. Successful hosting services may in the future host millions of objects on thousands of servers deployed around the globe, resulting in global information-hosting systems. Hosting services commonly use replication, or mirroring, to cope with load on popular web sites and to reduce bandwidth consumption in their backbones.

The project, the RaDaR (Replicator and Distributor and Redirector) architecture [20], is based on dynamic object replication and migration. While the idea of dynamic replication is by no means new, the context of the Internet presents important new challenges. First, two factors must be taken into account in a single framework: server load, and the proximity of clients to servers. Second, much of traditional work in dynamic replication has concentrated on protocol aspects, without considering the architecture. This project looks at the problem as a whole, paying special attention to architectural issues.

5.5.3.4 WebOS (http://www.cs.duke.edu/ari/issg/webos/)

Project Web Operating System (OS) began at the University of California, Berkeley in 1996 as part of the Network of Workstaions (NOW) project. It was completed in 1998 with the NOW finale. However, related efforts continued at member universities viz. Duke University (ISSG), the University of Texas at Austin (Beyond Browsers), and the University of

Washington. In addition, all three universities collaborated on the Active Names work that grew out of WebOS.

On a single machine, application developers can rely on the local OS to provide these abstractions. In the wide area, however, application developers are forced to build these abstractions themselves or to do without. This ad-hoc approach wastes programmer effort and system resources. To address these problems, WebOS attempted to develop a platform for providing basic OS services needed to build wide-area applications that are geographically distributed, highly available, incrementally scalable, and dynamically reconfiguring (such as PervComp). It would be able to support mechanisms for resource discovery, a global namespace, remote process execution, resource management, authentication, and security. An application that demonstrates the utility of WebOS is Rent-A-Server, a web server capable of dynamically replicating itself geographically in response to client access patterns.

The initial implementation was split into the following pieces: a) *WebFS*- a global file system layer allowing unmodified applications to read and write to the URL name space. Cache consistency would be available to applications requiring it through the AFS protocol, b) *Active Names*- a mechanism for logically moving service functionality such as load balancing, resource discovery, and fault transparency from the server into the network, c) *Secure Remote Execution*- since applications would be running on remote nodes on behalf of arbitrary users, assurances must be provided ensuring that applications were not able to violate the integrity of the remote server and that the servers could not take advantage of any user access rights provided to the programs, d) *Security and Authentication*- applications accessing remote files must authenticate their identities before access to protected files can be granted, and e) *Transactions*- applications must have well-defined failure modes. For example, an aborted remote agent should not leave a user's local file system in an inconsistent state.

5.5.3.5 Globus (http://www.globus.org/)

Project Globus is all about an infrastructure for global computing (i.e., a predecessor of PervComp). The development of the World Wide Web revolutionized the way we think about information. We take for granted our ability to access information from all over the world via the Web. The goal of the Globus project is to bring about a similar revolution with respect to computation that can be easily extended to PervComp. It is developing fundamental technologies needed to build *computational grids*. Grids are persistent environments that enable software applications to integrate instruments, displays, computational and information resources that are managed by diverse organizations in widespread locations. Grids support large user communities and are intended for use by scientists and engineers in a variety of disciplines. We can hardly imagine the types of applications we might construct if access to supercomputers, live satellite imagery, and mass storage were as straightforward as access to the Web. The Globus Project is developing the technology that can make this vision a reality (sounds similar to PervComp!).

Prototypes of computational grids are deploying the Globus Toolkit (a middleware) across a wide range of facilities and resources, including supercomputing centers, research labs, and college and university campuses. The goal is to build, operate, and encourage the use of a grid that will support distributed scientific and engineering applications and form the basis of a national computational infrastructure much in the same way that the NSFnet formed the basis of today's Internet. In February 2000, Globus Ubiquitous Supercomputing Testbed Organization (GUSTO) was created by a set of partners that included 125 sites in 23 countries, representing one of the largest computational environments ever constructed.

NASA Information Power Grid (IPG) is using the Globus Toolkit as a basis for joining supercomputers and storage devices owned by participating organizations into a single, seamless computing environment. Part of a joint effort among leaders within government, academia, and industry, the IPG will help NASA scientists collaborate to solve important problems facing the world in the 21st century. Just as the web makes information anywhere available everywhere, the IPG will someday give researchers and engineers around the country access to distant supercomputing resources and data repositories whenever they need them. The emerging computational Grid technologies (including those developed by the Globus Project) will be used by the European DataGrid project to establish a research network that will enable the development of the technology components essential for the implementation of a new worldwide data grid on a scale equivalent to that of PervComp. It will demonstrate: a) the effectiveness of this new technology through the large-scale deployment of end-to-end application experiments involving real users, and b) the ability to build, connect and effectively manage large general-purpose, data intensive computer clusters constructed from low-cost commodity components.

5.5.3.6 Cosm (http://www.mithral.com/projects/cosm/)

Publicly launched in March 1999, Cosm (Phase 1) is a framework for distributed computing applications through a set of open protocols and applications designed to allow computers all over the world to work together in distributed computing projects, or peer-to-peer applications. The project may be a mathematical challenge, or rendering an animation, or writing. Cosm also involves building the libraries, APIs, and standards that are required to make those types of applications easy to develop for every kind of system. The goal of Cosm is to build a stable, reliable, and secure system for large scale distributed processing. Clients should be "dumb" and only focus on ensuring that work they are given is completed by a core and returned. They should do this in a completely non-interfering way in the idle time of the host system. Command consoles should easily manage a group of clients run by a user without the need to visit each client physically beyond the initial installation or for the addition of new public keys. Proxies and servers should provide the infrastructure to serve the many clients.

5.5.3.7 XtremWeb (http://www.lri.fr/~fedak/XtremWeb/)

XtremWeb (XW) is another software platform for Internet Grid computing designed to serve as a substrate for Global Computing (Large Scale Distributed System) experiments. XtremWeb belongs to the so called Cycle Stealing Environment family that extends the principle of cycle stealing to the PC connected to Internet. XtremWeb is composed of Client, Servers and Workers. XtremWeb can be used to build a Global Computing System (such as PervComp) with centralized control, job scheduling and result collection. This architecture corresponds to most of well-known Global Computing Projects. Compared to some other platforms, XtremWeb also allows to connect several Servers and Result Collector on a single project (Workers keep a collection of Server and Result collectors IP address). During the execution, the workers contact the Server to get jobs. In response, the Server send a set of parameter and it also may send an application, if the application is not already stored in the Workers. When the Workers end their job, they contact the Result collector to send the results. Depending on the result size, the communication between the Workers and the Result Collector use different protocols. Currently, a Worker may send results up to 100 MBytes. In this architecture, the Client and the Server are the same computer.

XtremWeb can also be used to build centralized Peer-to-Peer (P2P) Systems, such as some well-known projects related to audio file exchange. However, currently, XtremWeb does not allow to store data on the Client/Worker resources. XtremWeb only allows P2P computing using the following design. Typically, one or several applications are downloaded on the Workers. Any Worker may submit jobs by contacting the P2P Server. In this case, the Worker behaves as a Client. Jobs submitted by Client are registered on the Server and scheduled on Workers. In this architecture, any Worker can be a Client. Currently, only trusted applications are allowed with this architecture. The next release of XW will encompass a sandboxing mechanism to protect the Worker of hackers attack. With this mechanism, any program may be submitted to the system and ran on a protected Worker. Note that the XtremWeb is not limited to centralized architectures and are currently being extended to a hierarchical design. Also, Workers may send their results directly to Clients to limit the bandwidth consummation.

5.5.4 Pervasive Computing

5.5.4.1 InConcert

As discussed in Chapter 1, there has been a strong initiative on middlewares in EasyLiving [9] project at Microsoft Research. For example, InConcert is a middleware solution that addresses the interfacing issues in EasyLiving. Also, there has been much research in EasyLiving regarding computer vision middlewares for tracking people [6].

By using the InConcert package, it is possible to develop new components for EasyLiving [9] relatively quickly. It provides asynchronous message passing, machine independent addressing and XML-based message protocols. Through asynchronous message passing, InConcert avoids blocking and inefficiency problems. Furthermore, an asynchronous approach allows programs to handle offline and queued operation more naturally. Clients are written to expect reply messages, if any are expected at all, to arrive at some arbitrary later time rather than as a return from the original request.

Inter-machine communication is handled by integrating a naming and lookup service into the delivery mechanism. When started, a component requests a name (an "Instance ID") and while running provides the lookup service with a periodic keep-alive message. The name is unique to this instance of the component; it remains constant even if the instance is stopped and later run on a different machine. Instance IDs are never reused. When sending messages, an instance includes its ID in the "From:" field of the message header. Receiving components can use that ID in the "To:" field of any response messages. When InConcert is asked to deliver the message, it will resolve the ID by asking the Instance Lookup Service for the instance's current location.

Descriptions of services are accomplished using a simple, open XML schema. In addition to ease of use, XML was chosen for two reasons. First, Extended Stylesheet Language (XSL) provides the ability to translate XML documents into multiple layouts. Second, it is straightforward to transform an XML-encoded description of a command into the XML-encoded command to be sent to the service. Once the message is delivered to the correct process, its content is decoded from the XML description. XML provides the ability to version each field and add additional information that, in other systems, would cause the endpoint binding to fail. As new parameters are supported on servers, clients can either omit or include the information. If the server requires the new field, then the error message returned can describe the exact field required rather than reporting a simple binding failure. This has made it possible to develop components that more accurately reflect the desired decomposition of interactions. It also allows components to be conveniently moved between hardware in order to tune the system performance. Finally, by designing the applications to handle asynchronous messages, the user experience is still responsive even when the device is isolated from all or part of the network.

5.5.4.2 omniORB

omniORB is an Object Request Broker (ORB), which implements specification 2.3 of the Common Object Request Broker Architecture (CORBA). It supports the C++ language binding; is fully multithreaded; uses IIOP as the native transport; and comes complete with a COS Naming Service. OmniORB is a robust, high-performance CORBA 2 ORB, developed by AT&T Laboratories Cambridge [21]. It is one of only three ORBs to be awarded the Open Group's Open Brand for CORBA. This means that omniORB has been tested and certified CORBA 2.1 compliant. omniORB implements the specification 2.3 of the Common Object Request Broker Architecture (CORBA). It is the third generation ORB (hence the name 'omniORB three'). The initial goal was to produce a standard conforming ORB that can deliver the performance required by the applications developed in-house. It has been deployed for lab-wide use since Mar 1997. In May 1997, the ORB was released externally as free software under the GNU Public Licenses.

5.6 SUMMARY

In summary, it appears that interfacing is a crucial job in PervComp as it has to adapt to a variety of differences both above and below itself. Many researchers propose that distributed event notification forms a fundamental requirement for systems of this scale. However, the current deployment of distributed systems is hampered by the close coupling of components through rigid interfaces. Direct, point-to-point binding of components inhibits runtime substitution, removal or addition of components.

In addition to limiting the interaction architecture of distributed systems to a client-server paradigm, the static definition of component interfaces using an IDL (such as ONC [15], DCE [4], CORBA [5], DCOM [1]) severely restricts the ability of applications to adapt to changes in their environment. An endpoint is bound directly to a component, and cannot be implemented by a group of cooperating objects nor can components simply extend their functionality to include new behavior. Their API effectively dictates the structure of applications. In a world of PervComp, where the applications architecture must adapt to the constantly changing environment, interfaces must be able to split and merge, run on a single machine or be spread across the world. Running applications must be able to constantly and seamlessly *adapt* to their current context.

As PervComp gets larger and more pervasive, they offer new opportunities. PervNet, connecting everything, starting from powerful high-performance machines and workstations to tiny pervasive devices, has an enormously powerful infrastructure that can solve pervasive problems and distribute huge amounts of information. Linked together, these connected resources make up a single, worldwide, virtual network. PervWare will provide an easy-to-use middleware that can manage this complex physical system and support large degrees of parallelism so that a virtual PervNet becomes a reliable, efficient, and real PervComp opportunity for a wide variety of users. Moreover, given current hardware trends and advances in virtual execution platforms, such as the Java virtual machine or Microsoft's common language runtime, we can reasonably expect that most devices can implement such a pervasive computing platform. Devices that do not have the capacity to implement the full platform, such as small sensors, can still interact with it by using proxies or emulating the platform's networking protocols.

REFERENCES

[1] Eddon Guy, et al. Inside Distributed COM, Microsoft Press, 1998.

[2] Thai Thuan L. Learning DCOM, O'Reilly and Associates, 1st Edition, April 1999.

[3] Java, http://www.java.sun.com/

[4] Sun Microsystems, Jini Distributed Event Specification, Technical Report, January 1999.

[5] Object Management Group, Common Object Request Broker: Architecture and Specification, OMG TC Document 91-12-1, December 1991.

[6] Box D, Ehnebuske D, Kakivaya G, Layman A, Mendelsohn N, Nielsen H. F, Thatte S, Winer D. Simple object access protocol (SOAP) 1.1. W3C note, World Wide Web Consortium, Cambridge, Massachusetts, May 2000.

[7] Universal Plug and Play, http://www.upnp.org/resources.htm

[8] Krumm John, et al. Multi-Camera Multi-Person Tracking for EasyLiving, Third IEEE International Workshop on Visual Surveillance, 2000; Dublin, Ireland.

[9] Shafer Steven, et al. The New EasyLiving Project at Microsoft Research. Proceedings of the 1998 DARPA / NIST Smart Spaces Workshop, July 1998.

[10] http://legion.virginia.edu/

[11] http://www.cs.duke.edu/ari/issg/webos/

[12] http://www.globus.org/

[13] http://www.mithral.com/projects/cosm/

[14] http://www.lri.fr/~fedak/XtremWeb/

[15] McManis Chuck and Samar Vipin. Solaris ONC: Design and Implementation of Transport-Independent RPC. Sun Microsystems, 1991.

[16] Satyanarayanan M. Scalable, Secure, and Highly Available Distributed File Access. IEEE Computer 1990; 9-21

[17] Satyanarayanan M. Coda: A Highly Available File System for a Distributed Workstation Environment. Proceeding 2nd IEEE Workshop on Workstation Operating Systems 1989, Pacific Grove, CA.

[18] http://www.infospheres.caltech.edu

[19] http://www.ece.purdue.edu/punch

[20] Rabinovich M, Aggarwal A. RaDaR : A Scalable Architecture for a Global Web Hosting Service. Computer Networks 1999.

[21] http://www.uk.research.att.com/omniORB.html

Chapter 6

Internet

There is no doubt that the Internet will be kernel of PervNet backbone (discussed in Chapter 3). So it is important to understand the Internet in minute details, after having some preliminary descriptions in Chapters 2 and 3. In particular, it is necessary to review the Internet protocol (IP) at length in order to estimate its potential to survive in the coming PervNet era.

6.1 INTRODUCTION

As discussed in Chapter 3, the development of PervNet infrastructure, one of the key requirements of deploying PervComp environment, will be based on a collection of heterogeneous networks. This, in turn, will tell us how to roam seamlessly around it and how to leverage computing in the PervNet infrastructure to enable new abilities and services for even the simplest pervasive devices [1]. Devices are heterogeneous, ranging from wearable devices to conventional computers. Moreover, wireless networking standards provide local connectivity for mobile nodes, while the Internet provides worldwide connectivity. Thus, PervNet will have to deal with a wide spectrum of traffic characteristics. The Internet is the prime component to constitute the core of PervNet infrastructure in the PervComp environment. This infrastructure could rely on the concept of packet switching offering the highest degree of flexibility to meet the different application requirements because it already connects the millions of users. The full IP integrated network architecture together with wireless domains will be the provision in the PervNet environment.

We have already seen in Chapter 3 that the development of high bandwidth PervNet infrastructure is being led by the development of terabit-speed routers and the development of Dense Wave Division Multiplexing

(DWDM) optical technologies. The introduction of multiprotocol label switching (MPLS) and its extensions to multiprotocol lambda switching (MPλS)/generalized MPLS (GMPLS) in the extension of IP suite of protocols will be the seed of major transformations in the core network infrastructure [2]. The core infrastructure will be developed with IP/MPLS and the optical layer as the predominant networking layers. This implies that the bulk of transport, switching, multiplexing, and routing functions will be performed only at those layers. The success of IP technology is founded, among other factors, on the wide diversity of link layer and lower layer protocols supported by the IP protocol. This diversity will continue, but it is very likely that Ethernet and SONET/SDH will be the predominant framing layers for the core infrastructure of PervNet (as outlined in Chapter 3).

PervNet infrastructure also critically depends on the design and deployment of a unifying control plane, built around IP and MPLS control protocols. DWDM optical transmission techniques permit multiple signals to be transmitted on a single optical fibre using different wavelengths of light. In order to achieve higher levels of router performance, much of the logical functions is being moved from software running on general-purpose microprocessors to custom-built Application-Specific Integrated Circuits (ASICs). The Internet on this infrastructure will provide a new set of capabilities, not present in current IP backbone networks, for the dynamic provisioning of optical bandwidth upon request of IP routers and label switched routers (LSRs). This feature will stretch the possibilities of the Internet in terms of dynamic behaviour and service flexibility, which are two prime requirements of PervNet. New control interfaces, between routers and optical networks, will be developed to support this capability.

The IP backbone in PervNet will have to accommodate a global number of users that who connect at faster data rates due to the widespread use of DSL, cable modems, and 3G/4G mobile services [2]. But the PervNet infrastructure is not only about more bandwidth; it is about new service models and richer services of quality of service (QoS). The differentiated services (DiffServ) architecture approaches the problem of QoS support from the point of view of allowing for controlled unfairness in the use of network resources. The DiffServ architecture aims at providing simple and scalable service differentiation by recognizing that most data flows generated by different applications can ultimately be classified into a few general categories (i.e., traffic classes). A combination of DiffServ and MPLS mechanisms will be deployed to ensure QoS across networks.

In the PervNet infrastructure, the mobile network has functioned as an access gate to the Internet for giving mobile Internet services to users. It is currently predicted [3] that IP traffic will dominate and voice traffic will decrease in the mobile network. Moreover, IP is being improved to support voice also. This means that all traffic in the mobile network will be IP-based in the near future. Therefore, the mobile network must efficiently transport IP traffic in the next phase, that is, beyond IMT-2000. The third-generation (3G) system known as the IMT-2000 will enhance the ability of data communications. The mobile communications system beyond IMT-2000 (4G) should be designed to offer significantly higher bit rates than even in a vehicular environment and to adapt to data communications more efficiently to realize the concept of "every time, everywhere, everyone, and everything" from the viewpoint of pervasive and ubiquitous computing. The IP, already a universal network layer protocol for wireline packet networks, is becoming universal network layer protocol over all wireless systems. An IP device would roam different wireless systems if they all support IP as a common network layer in PervNet infrastructure. The IP provides a globally successful open infrastructure for different QoS-based services and applications to information users.

In the PervComp, users will exchange information and control their environments from a where using various wireline/wireless networks and pervasive devices [4]. The current wireline/wireless protocols, such as IP protocol suite with extensions, Mobile IP/Cellular IP in their present and/or enhanced forms would be used to support PervNet access for data networking. In addition, the structure of IP to support voice in PervNet would be addressed.

6.2 IPV6

6.2.1 Basic Structure

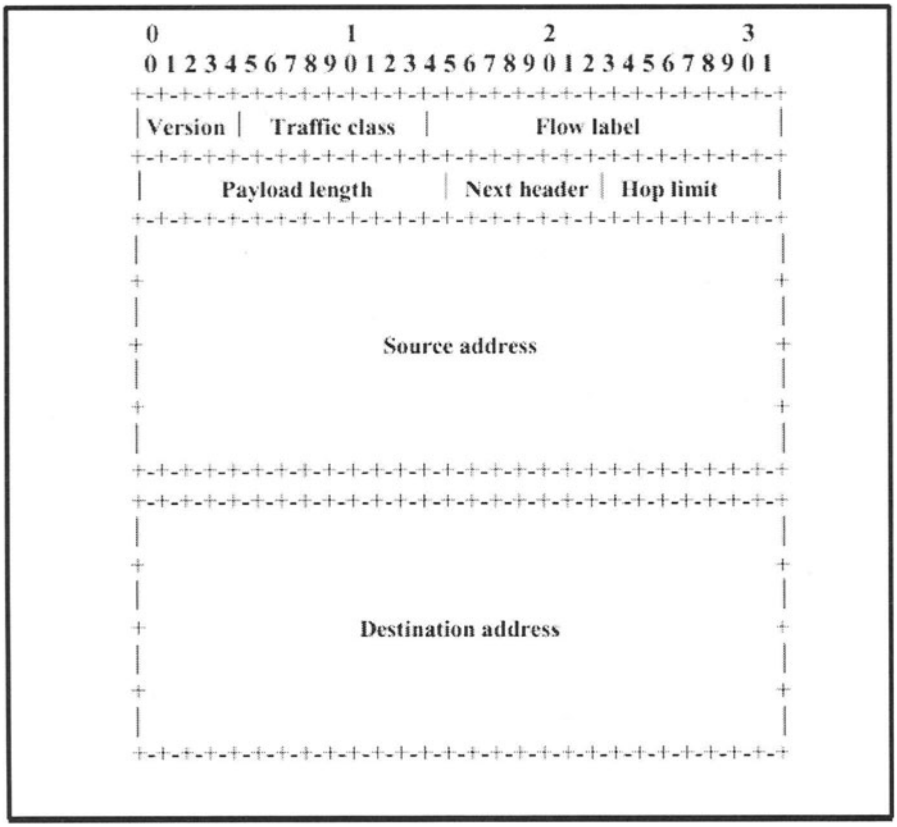
IP is the protocol, which provides packet routing and delivery services for the Internet, and IP version 6 (IPv6) is a new version of IP intended to replace the current version of IP (IPv4) [5] [6]. IP provides the functionality for interconnecting end systems across multiple networks. For this purpose, IP is implemented in each end system and in routers, which are devices that provide connection between networks. Higher-level data at a source end system are encapsulated in an IP protocol data unit (PDU) for transmission. This PDU is then passed through one or more networks and connecting routers to reach the destination end system.

The driving motivation for the adoption of a new version of IP was the limitation imposed by the 32-bit address field in IPv4. In addition, new requirements in the areas of security, routing flexibility, and traffic support have developed in this version of IP.

IPv6 exhibits a number of changes from IPv4: *Expanded address capabilities*: IPv6 uses 16-byte-long addresses; these extend the Classless Interdomain Routing (CIDR) addressing hierarchy strategy and definitively overcome the scaling problem of IPv4 (which uses 4-byte-long addresses).

New packet format: The packets are based on a simple header. Also, the way header options are encoded has been totally improved. *Multicast support*: IPv6 supports multicast as a native communication mode. Moreover, the addition of a scope field to multicast addresses improves the scalability of multicast routing. *Flow labelling capability*: This allows a sender to identify packets as being related to one another (i.e., belonging to the same traffic flow).

Anycast support: Anycast is used to send a packet to any one member of a group of receivers. *Authentication and privacy capabilities*: It includes the definition of extensions, which provide support for authentication, data integrity, and confidentiality.



```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|Version| Traffic class |           Flow label                  |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|         Payload length        |  Next header  |   Hop limit   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
+                                                               +
|                                                               |
+                         Source address                        +
|                                                               |
+                                                               +
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
+                                                               +
|                                                               |
+                      Destination address                      +
|                                                               |
+                                                               +
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 6.1 IPv6 Header Format

The most visible difference is that IPv6 addresses are all 128 bits long, instead of 32 bits long as in IPv4. Within this huge address space, a tiny part is reserved for all current IPv4 addresses, and another tiny part is reserved for the Link-Local addresses, which are not routable but which are guaranteed to be unique on a link i.e., on a local network. Nodes on the same link can communicate with each other even without any routers, by using their Link-Local addresses. Nodes discover each other's presence, as well as each other's link-layer i.e., MAC addresses, by participating in the Neighbor Discovery protocol; IPv6 nodes also discover local routers and network prefixes by means of Neighbor Discovery. The IPv6 Neighbor Discovery protocol can be characterized as a much-improved version of two IPv4 protocols, the Address Resolution Protocol (ARP) and the Internet Control Message Protocol (ICMP) Router Discovery Protocol. IPv6 defines several kinds of extension headers, which may be used to include additional information in the headers of an IPv6 packet. The defined IPv6 extension headers include: *Destination Options header, Hop-by-Hop Options header, Routing header, Fragment header and Authentication header.*

Destination header is used to carry information that needs to be examined and processed by the destination of the packet. Hop-by-hop options header carries information that has to be examined and processed by each node on the packet's path, with the source and destination included. In IPv4, every IP option is treated essentially as a Hop-by-Hop option and thus causes performance degradation because of processing needed at every intermediate router, whether it pertains to that router or only to the final destination node. Routing header is used by a source to list one or more routers to be visited by the packet en route to its destination. This is very similar to IPv4's source route option. The IPv6 Routing header can serve both as a strict source route and a loose source route. Unlike the IPv4 Source Route options, however, in IPv6, the Routing header is not examined or processed until it reaches the next node identified in the route. In addition, the destination node receiving a packet with a Routing header is under no obligation to reverse the route along which the packet was received, for routing packets back to the sender. Fragment header is used when fragmentation is required. In IPv6, fragmentation can only be done at the source. The Authentication header provides a means by which a packet can include optional authentication data, for example based on a one-way cryptographic hash (e.g., MD5) of the packet's contents. The inclusion of this authentication data allows the receiver to verify the authenticity of the packet sender, and also protects against modification of the packet while in transit, since a modified packet will be viewed by the receiver the same as a forged packet. The Authentication header may also be used to provide re-play protection of packets, such that an attacker cannot later resent saved copies of an authenticated packet.

6.2.2 Mobility in IPv6

Mobile IPv6 is intended to enable IPv6 nodes to move from one IP subnet to another [7]. The protocol allows a mobile node to communicate with other nodes (stationary or mobile) after changing its link-layer point of attachment from one IP subnet to another, yet without changing the mobile node's IPv6 address. A mobile node is always addressable by its home address, and packets may be routed to it using this address regardless of the mobile node's current point of attachment to the Internet. Each IPv6 node is permanently identified by its *home address*. When a mobile node leaves its home subnet, it leaves a *care-of address* behind with a *home agent*. The home agent is a router responsible for intercepting packets bound for the home address of the mobile node and encapsulating them for tunnelling to the care-of address. This preserves transparency of location to all higher protocol layers and corresponding hosts. The movement of a mobile node away from its home subnet is thus transparent to transport and higher-layer protocols and applications.

Each time the mobile node moves its point of attachment from one IP subnet to another, the mobile node will configure its care-of address by stateless address autoconfiguration, or alternatively by some means of stateful address autoconfiguration such as DHCP or PPP. The decision about which manner of automatic address configuration to use is made according to the methods of IPv6 Neighbour Discovery. A mobile node may have more than one care-of address at a time, for example if it is link-level attached to more than one (wireless) network at a time or if more than one IP network prefix is present on a network to which it is attached. It is then responsible for sending this care-of address back to its home agent (router). The route acting as home agent uses proxy Neighbour Discovery to intercept packets for the mobile node. The link by which a mobile node is directly attached to the Internet would often be a wireless link. All packets used to inform another node about the location of a mobile node must be authenticated. Also, the number of administrative packets sent over the link by which a mobile node is directly attached to the Internet should be minimized, and the size of these packets should be kept as small as is reasonably possible. This means that route optimisation fits naturally within the framework offered by IPv6. Since future Internet nodes are expected to be capable of mobility, this represents a significant reduction in the network load to be sustained by the IPv6 Internet.

Any sender that has the mobile node's care-of address uses a routing header (the IPv6 equivalent of source routing) in order to send packets to the mobile node. On the other hand, whenever a packet arrives at the home agent instead of going directly to the mobile node, it can be assumed that the sender does not have the care-of address of the mobile node. In this case, the home agent does not insert a source route to complete the delivery of the packet to the mobile node. Instead, the home agent is required to use encapsulation. Thus, the mobile node can tell whenever it needs to send a binding update to any of its correspondents. Moreover, when the mobile node moves to a new care-of address, it assumes that each of its active correspondent nodes should receive a new binding update. The mobile node can find active correspondent nodes by checking its TCP protocol control blocks; but this only works for TCP traffic.

6.3 MOBILE IP

6.3.1 Basics of Mobile IP

Mobile IP provides an IP-based mobility solution that allows mobile nodes (MNs) to maintain network connectivity while retaining their permanently assigned IP addresses [8]. In particular, it enables the mobility of a user to be transparent to all executing applications. This is essentially achieved by providing the mobile with an address (in addition to its permanent address) that is topologically consistent. This address is referred to in the foreign network as the *care-of address*, and ensures that packets are forwarded using conventional IP routing to the mobile's current location in the foreign network. In Mobile IP, the *home address* is static and is used, for instance, to identify TCP connections. The *care-of address* changes at each new point of attachment and can be thought of as the mobile node's topologically significant address; it indicates the network number and thus identifies the mobile node's point of attachment with respect to the network topology. The home address makes it appear that the mobile node is continually able to receive data on its *home network*, where Mobile IP requires the existence of a network node known as the *home agent* (HA). Whenever the mobile node is not attached to its home network (and is therefore attached to what is termed a *foreign network*), the home agent gets all the packets destined for the mobile node and arranges to deliver them to the mobile node's current point of attachment. Whenever the mobile node moves, it *registers* its new care-of address with its home agent. To get a packet to a mobile node from its home network, the home agent delivers the packet from the home network to the care-of address. The further delivery requires that the packet be modified so that the care-of address appears as the destination IP address. This modification can be understood as a packet transformation or, more specifically, a *redirectio*n. When the packet arrives at the care-of address, the reverse transformation is applied so that the packet once again appears to have the mobile node's home address as the destination IP address. When the packet arrives at the mobile node, addressed to the home address, it will be processed properly by TCP or whatever higher-level protocol logically receives it from the mobile node's IP (that is, layer 3) processing layer. In Mobile IP the home agent redirects packets from the home network to the care-of address by constructing a new IP header that contains the mobile node's care-of address as the destination IP address. This new header then shields or encapsulates the original packet, causing the mobile node's home address to have no effect on the encapsulated packet's routing until it arrives at the care-of address. Such *encapsulation* is also called *tunnelli*ng, which suggests that the packet burrows through the Internet, bypassing the usual effects of IP routing. Mobile IP, then, is best understood as the cooperation of three separable mechanisms: Discovering the care-of address; Registering the care-of address; Tunnelling to the care-of address.

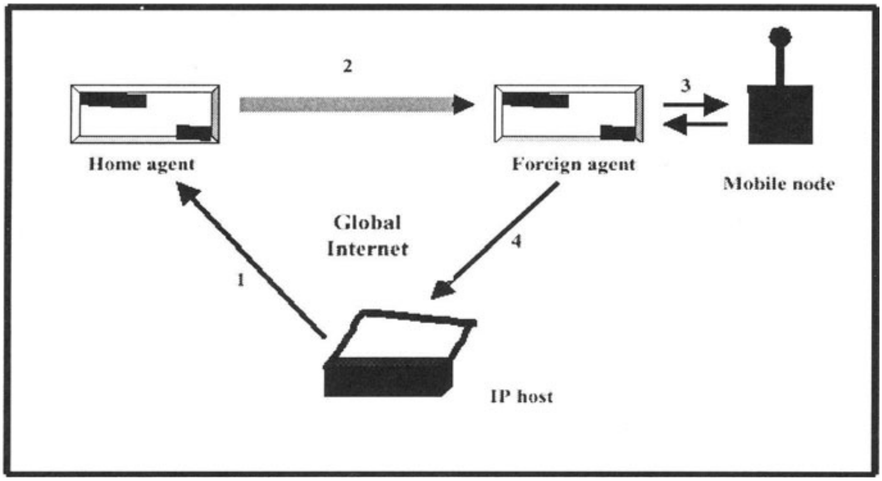


Figure 6.2 *Data Flow in Mobile IP Protocol*

The basic Mobile IP specification allows for two distinct methods of operation:

- The first mode of operation uses a *foreign agent* (FA) while visiting the foreign network (a network other than the MN's home net-work). The FA provides the mobile with a binding (IP address) that is consistent with the addressing scheme deployed in the foreign network. An MN can connect to the foreign network by registering the IP address of the FA with its HA, statically assigned to the MN in its home network.

The second mode of operation does not require any agent support in the foreign network but requires MNs to obtain a temporary IP address therein. The MN usually obtains this address from a specified pool using protocols such as Dynamic Host Configuration Protocol (DHCP), and then uses its own collocated care-of address in the foreign network. The collocated address mechanism allows the MN to have direct control over the path of its own packets, and also does not rely on the existence of additional agents in the foreign network. The basic operational mode of Mobile IP architecture gives rise to the phenomenon of *triangular routing*: while packets from the MN usually follow a direct path to the *correspondent nodes* (CNs), packets from the CNs are rerouted via the MN's home net-work to its point of attachment in a foreign network, from where they are forwarded to the MN' s current location. The route optimisation protocol eliminates the triangular routing by essentially transmitting binding messages directly to CNs. While this form of route optimisation will result in significant bandwidth savings by eliminating unnecessary path traversals, especially as the number of MNs increases, also it can give rise to significantly high latency during the location update process. However, the route optimisation, at least in some modified form, is essential for supporting real-time communications in any future mobility- enhanced network infrastructure.

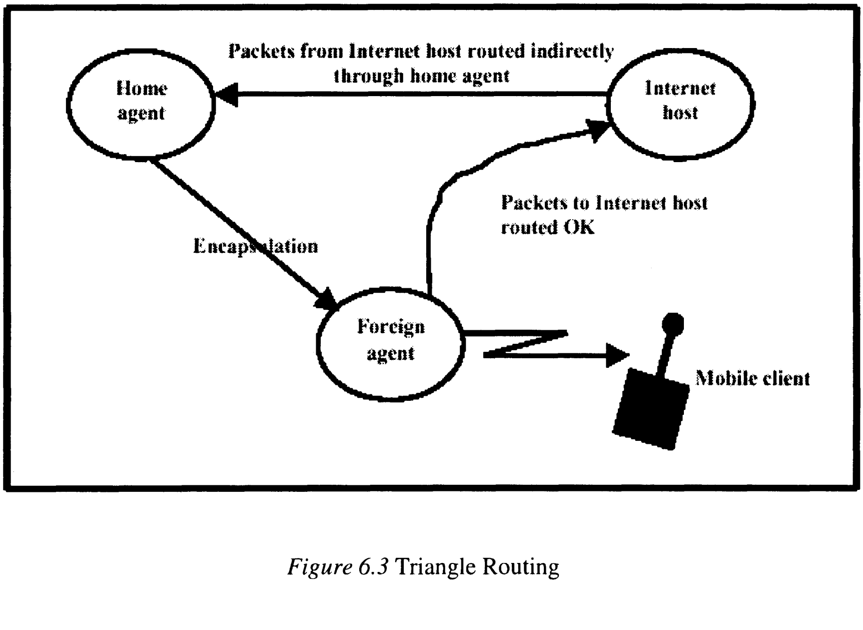

Packets from Internet host routed indirectly through home agent
Home agent
Internet host
Packets to Internet host routed OK
Encapsulation
Foreign agent
Mobile client

Figure 6.3 Triangle Routing

6.3.2 Mobile IP with AAA

The extension of Mobile IP is possible for its use in cellular telephone networks, a few number of additional mechanisms are needed to incorporate in the existing protocol by which the agent at the point of connection on the foreign domain (the foreign agent) can verify the identity of the mobile node, and also authorize connectivity based on local policy or ability to pay. These extensions rely on the existence of servers that are capable of performing three services: *accounting*, *authentication*, and *authorization* (*AAA*) [9]. The AAA extensions in Mobile IP will create a more acceptable path toward ubiquitous availability of wireless service for many different wireless access services across the domain boundaries of the operators.

The users have Internet services by obtaining a point of attachment to a home domain, generally from an Internet service provider (ISP) or some other organization. With the increasing usage of different mobile devices, it is necessary to allow users to attach to any domain convenient to their current location; any user often needs access to resources provided by an administrative domain other than their home domain (i.e., a foreign domain). Service providers in a foreign domain commonly require authorization to ensure authenticity of the users. This leads directly to authentication, and subsequently accounting; these three AAA functions are closely interdependent. An agent in the foreign domain that attends to the user's request (called the *attendan*t) checks user's authenticity and, in turn, give access to resources after the authentication of the user's is valid. The attendant may not have direct access to the data to complete the transaction. Instead, the attendant is expected to consult a local authority in the same foreign domain in order to obtain proof that the client has acceptable credentials.

Since the attendant and the local authority are part of the same administrative domain, they are expected to have security relationships that enable them to securely transact information locally. The local authority in the foreign domain (*AAAF*) itself may not have enough information to verify the credentials of the client. Nevertheless, in contrast to the agent attending the user, AAAF is configured to be able to negotiate the verification of user credentials with an external authority (e.g., *AAAH*). The local and external authorities are configured with sufficient security relationships and access control so that they, possibly without the need for any other agents, can negotiate the authorization, which enables the user to have access to the requested resources. This authorization commonly depends on secure authentication of the client's credentials. Once the local authority has obtained the authorization, and the authority has notified the attendant of the successful negotiation, the attendant can provide the requested resources to the client.

For Mobile IP, the AAA server has the following additional general tasks:

- Authorize the MN (once its identity has been established) to use Mobile IP and certain specific services
- Initiate and enable the authentication for Mobile IP registration
- Distribute keys to the MN and mobility agents

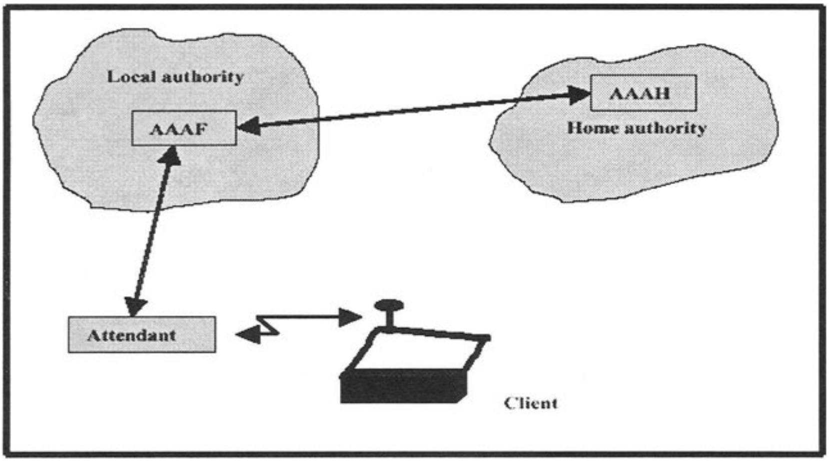


Figure 6.4 Servers in Foreign and Home Domains

The lifetime of any security associations distributed by the AAA server for use with Mobile IP should be long enough to avoid too-frequent initiation of AAA key distribution, since each invocation of this process is likely to cause lengthy delays between registrations. Registration delays in Mobile IP cause dropped packets and noticeable disruptions in service. The lifetime of the key between the MN and the HA can just as well determine the length of time before the MN has to initiate a new key distribution from the AAA servers. The major difference for IPv6 is that the natural repository for the attendant (the FA) is no longer part of the protocol model. Instead, the analogous attendant functionality will become associated with either IPv6 routers or stateful configuration services.

6.3.3 Macro Mobility in Mobile IP

A various number of solutions have been proposed [10] to handle Mobile-IP-based mobility management problems, such as firewall traversal

[11], or reverse or bi-directional tunnelling [12]. These proposed solutions are still not particularly suitable for supporting macro mobility in cellular wireless networks. They lack support for fast handoff control, real-time location update, registration, and configuration. Moreover, the importance of application-transparent mobility has diminished in present scenarios since many applications (e.g., Web browsing) are now able to internally handle network-level mobility. An extension to Mobile IP uses hierarchical FAs to handle macro-mobility [13]. In this architecture, BSs are assumed to be network routers; hence, it is not compatible with current cellular architectures, in which BSs are simply layer 2 forwarding agents. Moreover, deploying a hierarchy of FAs brings with it complex operational and security issues and requires multiple layers of packet processing on the data transport path. The presence of multiple layers of mobility-supporting agents also significantly increases the possibility of communication failure, since it does not exploit the inherent robustness of Internet routing protocols.

Handoffs are built on top of the mobile routing capabilities of Mobile IP. Mobile hosts connect to a wired infrastructure via base stations (BSs), which act as foreign agents. A home agent encapsulates packets from the source and forwards them to the BSs. The mobile selects a small group of BSs to listen to this multicast address for packets forwarded by the HA. One of the BSs is selected by the MH to be a *forwarding* BS; it decapsulates the packets sent by the HA and forwards them to the MH. The others are *buffering* BSs; they hold a small number of packets from the HA in a circular buffer. BSs send out periodic beacons similar to Mobile IP foreign-agent advertisements. The MH listens to these packets and determines which BS should forward packets, and which should buffer packets in anticipation of a handoff; the rest simply don't listen to the multicast group at all. When the mobile initiates a handoff, it instructs the old BS to move from forwarding to buffering mode and the new BS to move from buffering to forwarding mode. The new BS forwards the buffered packets that the mobile has not yet received. The MH decides that the current network is unreachable and hands over to the next higher network. A hierarchy exploits the geographic locality inherent in user mobility patterns. The lowest level of the hierarchy optimises the common case of movement between adjacent cells in the same network. It operates in the area near the mobile node and handles such motion without involving the mobile node's home network. The higher levels of the hierarchy rely on a general mechanism like Mobile IP to handle the less frequent movement between subnetworks or administrative domains (macro level). To handle motion within an administrative domain, the extending Mobile IP includes a hierarchy of foreign agents.

Several IETF proposals [14] [15] have also explored the possibility of using hierarchical FAs for seamless mobility within a domain. The need for hierarchical agents in Internet mobility architecture remains an open issue. A recent draft on Mobile IP regional tunnel management was proposed in the IETF. The proposal provides a scheme for performing registrations locally in the visited (foreign) domain, thereby reducing the number of signalling messages forwarded to the home network as well as lowering the signalling latency that occurs when an MN moves from one FA to another.

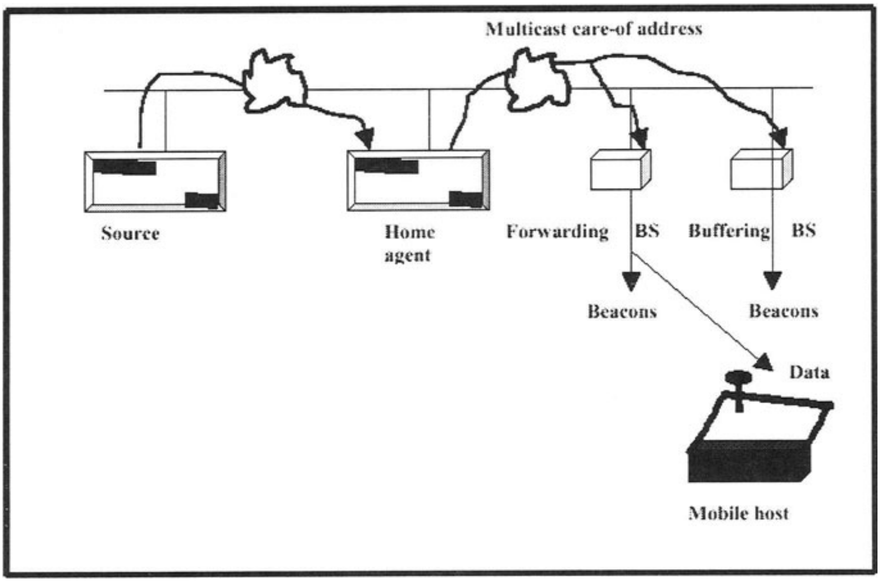


Figure 6.5 Elements of Hand-off System

The suggested enhancement to the registration scheme uses a gateway FA (GFA), which lays one level higher in the FA hierarchy, provides a stable global care-of address to the MN, and is supporting fast micro mobility management. At the top level, there are one or several GFAs, and on the lower level, there are a number of foreign agents. The structure can be extended to include multiple hierarchy levels of foreign agents beneath the GFA level. The security associations have been established between a GFA and all the foreign agents beneath it in the hierarchy. When a mobile node performs registration at its home network, registration keys are generated and distributed to the mobile node and to the GFA. The GFA may then in turn distribute the registration keys to the foreign agents beneath it in the hierarchy. If the distance between the visited network and the home network of the mobile node is large, the signalling delay for these registrations may be long. By registering locally within a visited domain, the signalling delay is reduced. These registrations reduce the number of signalling messages to the home network, and reduce the signalling delay when a mobile node moves from one foreign agent to another, within the same visited domain.

6.3.4 HAWAII

The Handoff-Aware Wireless Access Internet Infrastructure (HAWAII) [16] proposes a technique for using a separate binding protocol to handle intradomain mobility while using Mobile IP for interdomain mobility. It suggests the use of a two-layer hierarchy for mobility management. When the MN moves into a foreign domain, it is assigned a collocated care-of address from that domain, and the MN retains its care-of address unchanged while moving within the foreign domain. Thus, the movement of the MN within a domain is transparent to the HA. This protocol uses path setup messages to establish and update host-based routing entries for MNs in some specific routers within the domain; other routers not in the path are kept in the dark about the MN's new care-of address. When a CN sends packets to a roaming user, it uses the MN's home IP address. The HA intercepts the packets and sends the encapsulated packet to the MN's current border router. The border or root router decapsulates and again encapsulates the packet to forward it to either the intermediate router or BS, which decapsulates the packet and finally delivers it to the MN. This is illustrated in Figure 6.6.

6.3.5 Wireless IP

Another framework for IP-based mobility management was recently developed by the Telecommunications Industry Association (TIA) Standards Subcommitte TR45.6 [17] to target 3G cellular wireless systems. The International Telecommunication Union (ITU) has set the requirements for IMT-2000. The framework uses Mobile IP with FAs for inter-domain or global mobility. For intradomain or macro-mobility, the scheme proposes the use of dynamic HAs (DHAs), which reside in the serving network and are dynamically assigned by the visited authentication, authorization, and accounting (AAA) server. The DHA allows the roaming user to gain service with a local access service provider while avoiding unnecessarily long routing. The architecture defines a new node called a *packet data serving node* (PDSN) (which contains the FA), and uses VLR/home location register (HLR) (ANSI-41 or GSM-MAP) authentication and authorization information for the access network. The mobile node is identified by a network access identifier (NAI) [18] in the visiting or foreign network. An MN sends the registration to the FA, which in turn interacts with an AAA server residing in that network or uses the broker network for authentication with the home network.

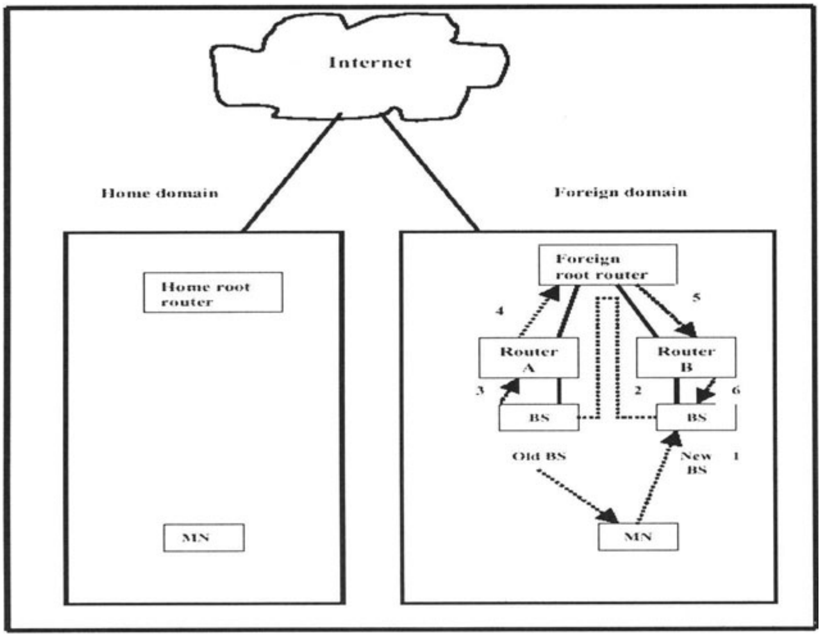


Figure 6.6 Mobility using HAWAII architecture

6.4 CELLULAR IP

Cellular IP proposes an alternative method [19] [20] to support local mobility (micro- and macro-mobility) in a cellular network, which consists of interconnected cellular IP nodes. Cellular IP makes use of layer-2 information regarding access point signal strength in order to predict handover, allowing the terminal to trigger layer-3 procedures earlier. Each Cellular IP domain is composed of a number of Cellular IP nodes structured in a tree topology, having a Mobile IP gateway as the root node. In particular, Cellular IP is designed to support local mobility, say, between BSs in a cellular network. Since MN addresses have no location significance inside a Cellular IP network, the architecture uses the home IP address as a unique host identifier. When an MN enters a Cellular IP network, it communicates the local gateway's (GW's) address to its HA as the care-of address. Nodes outside the Cellular IP network do not need any enhancements to communicate with nodes inside the network. The base stations are built on regular IP forwarding engines, but Cellular IP routing and location management, in turn, replaces IP routing. Mobile IP manages mobility between gateways (i.e., among Cellular IP networks) while Cellular IP handles mobility within access networks. When a CN sends packets to a roaming user, it uses the MN's home IP address. As in conventional Mobile IP, the HA intercepts the packets and sends the encapsulated packet to the MN's current GW. The GW decapsulates the packet and forwards it to the MN's home address using a node-specific route. Thus, the nodes sending or receiving datagrams to/from the MN remain unaware of the node's location inside the Cellular IP network.

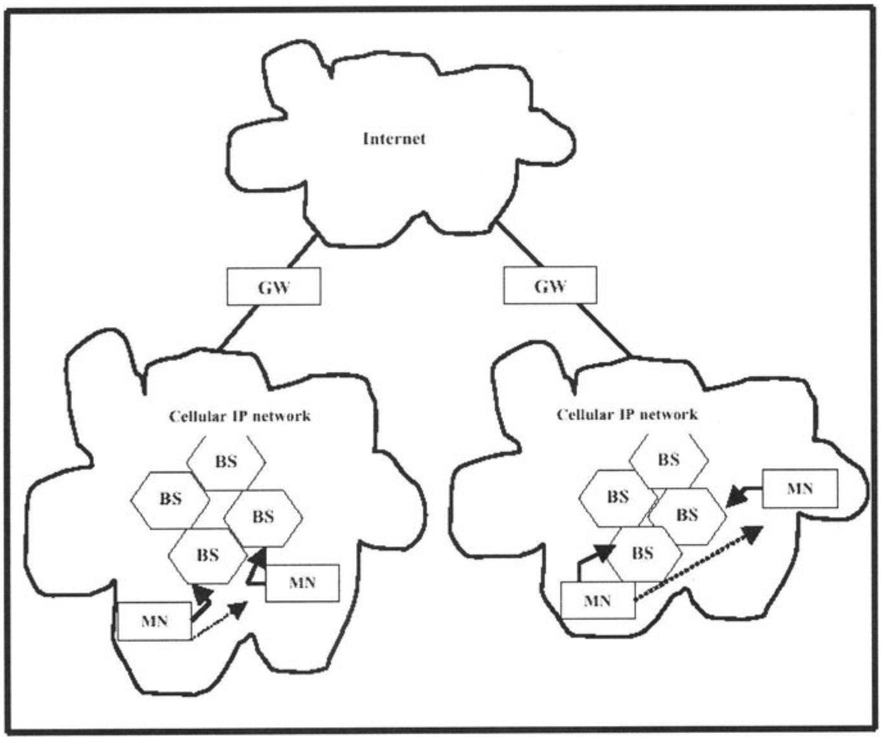


Figure 6.7 Mobility in Cellular IP Networks

Within the Cellular IP domain, when the terminal approaches a new BS, it redirects its outgoing packets from the old BS to the new BS, updating the routing caches all the way up to the gateway. All packets destined to the mobile terminal are forwarded to both BSs during a time interval equal to the routing cache timeout. After the old path expires, the packets destined to the mobile terminal are only forwarded to the new path. As such, when the terminal has no packets to send during handover, it has to generate route-update messages in order to allow correct updating of the routing caches. To minimize control messaging, regular data packets transmitted by mobile hosts are used to establish host location information. Uplink packets are routed from mobile to the gateway on a hop-by-hop basis. The path taken by these packets is cached in base stations. To route downlink packets addressed to a mobile host the path used by recent packets transmitted by the host is reversed. When the mobile host has no data to transmit then it periodically sends empty IP packets to the gateway to maintain its downlink routing state. Following the principle of passive connectivity mobile hosts that have not received packets for a certain period of time allow their downlink soft-state routes to timeout and be cleared from the routing cache. In order to route packets to idle hosts a Cellular IP mechanism called paging is used. Between Cellular IP domains, normal Mobile IP procedures are used for macromobility. In Cellular IP, all packets generated within the Cellular IP domain must be routed by the gateway, even if the destination is located in a position adjacent to the source.

6.5 CORE IP NETWORKS

6.5.1 Internet Service Architecture

The IP core networks in the PervNet architecture will have to accommodate a global number of users, and who connect at faster data rates due to the widespread use of DSL, cable modems, and future 3G mobile services [21]. This global communication network will not only have to cope with the amount of traffic generated by the tremendous number of anticipated users, but will also have to deal with a wide spectrum of traffic characteristics. This is because the network will have to support, simultaneously, applications that have a wide range of expectations and requirements. Among the networks available today, those based on the concept of packet switching offer the highest potential degree of flexibility to meet the different application requirements, and therefore offer the best available technology on which the PervNet infrastructure could rely. Because it already connects millions of users, the Internet is the uncontested prime candidate to constitute the core of a global infrastructure. The future Internet is not only about more bandwidth; it is about new service models and richer services [21]. The flat best-effort service provided by the present network may not be the most appropriate any longer: users requiring the assurance of better quality of service (QoS). As many real-time applications have been developed in the Internet, the best effort delivery model became inadequate for these new applications. Two different models are proposed to guarantee QoS in the Internet by the Internet Engineering Task Force (IETF): the integrated services (IntServ) and differentiated services (DiffServ) models. In the IntServ model, network resources are explicitly identified and reserved. Network nodes classify incoming packets and use reservations to provide QoS. In the DiffServ model, resources are not explicitly reserved. Instead, traffic is differentiated into a set of classes, and network of the most successful protocol, IPv4, allows DiffServ-style QoS to be applied. Some applications, such as streaming audio and video, would be much better served under the IntServ model since they have a relatively constant bandwidth requirement for a known period of time.

TCP, used widely in the current Internet [27], is not well suited to real-time applications. Instead, Real-Time Transport Protocol (RTP) is usually implemented on top of UDP, which is better adapted to real-time applications. This protocol mechanism is not enough to guarantee a specific quality of service (QoS) for a session between a sender and a receiver. Resource Reservation Protocol (RSVP) is an attempt to provide real-time service through the use of virtual circuits. It is a resource reservation setup protocol designed for the IntServ model. RSVP is not a routing protocol but a control protocol, which allows Internet real-time applications to reserve resources before they start transmitting data. That is, when an application invokes RSVP to request a specific end-to-end QoS for a data stream, RSVP selects a data path relying on underlying routing protocols, and then reserves resources along the path. Since RSVP is also receiver-oriented, each receiver is responsible for reserving resources to guarantee requested QoS along its data path. The receiver sends a message to reserve resources along all the nodes on the delivery path to the sender.

The DiffServ architecture [22] aims at providing simple and scalable service differentiation by recognizing that most data flows generated by different applications can ultimately be classified into a few general categories (i.e., traffic classes). It does this by discriminating and treating the data flows according to their traffic class, thus providing a logical separation of the traffic into the different classes. A combination of DiffServ and Multiprotocol label switching (MPLS) mechanisms will be deployed to ensure QoS across intradomain and interdomain networks [2]. Another major transformation in the upcoming Internet will be the widespread use of virtual private network (VPN) services, enabled by a very scalable solution that combines MPLS and Border Gateway Protocol v.4 (BGP4) [23]. This solution places no constraints on addressing plans used by VPNs, and provides basic security comparable to that provided by frame relay or asynchronous transfer mode (ATM)-based VPNs, but without incurring the overhead and complexity associated with the use of overlay models or IPSec. MPLS, an extension to the existing IP architecture and by adding new capabilities to the IP architecture, MPLS enables support of new features and applications, the differences between MPLS and traditional IP routing and forwarding. The new applications include traffic engineering, IP virtual private networks, integration of IP routing and layer 2 or optical switching, and other applications. The overlap in technology means that there is much in common between the process of design of MPLS networks and the design of other IP routed networks.

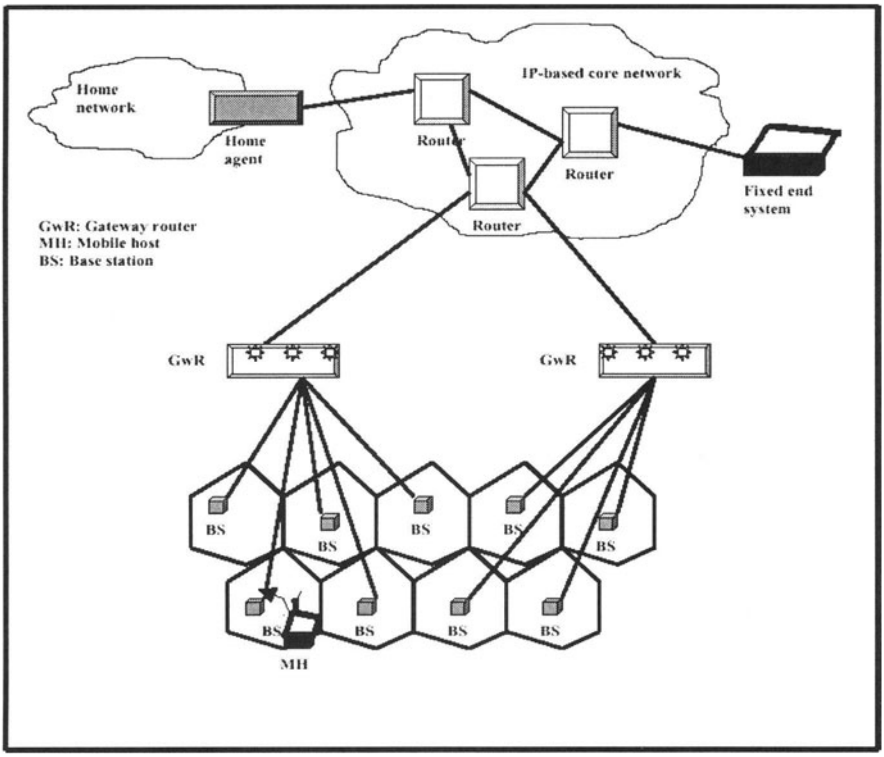


Figure 6.8 IP core networks

The future Internet [2] will be built with IP/MPLS and the optical layer as the predominant networking layers. This implies that the bulk of transport, switching, multiplexing, and routing functions will be performed only at those layers. The success of IP technology is founded, among other factors, on the wide diversity of link layer and lower layer protocols supported by the IP protocol. This diversity will continue, but it is very likely that Ethernet and SONET/SDH will be the predominant framing layers for the optical Internet. MPLS will provide the capabilities required to deploy feature-rich data services, to an arguable extent displacing ATM. The future Internet also depends on the design and deployment of a unifying control plane, will be built around IP and MPLS control protocols. This Internet will also provide a new set of capabilities, not present in current IP backbone networks, for the dynamic provisioning of optical bandwidth upon request of IP routers and label switched routers (LSRs). This feature, also known as *optical bandwidth on deman*d, will stretch the possibilities of the optical (future) Internet in terms of dynamic behaviour and service flexibility. New control interfaces known as the *optical user–network interface*, between routers and optical networks, support this capability. Recently, as it becomes easier to access the Internet from a mobile host, mobile users are demanding the same real-time service available to fixed hosts. Mobility of hosts has a significant impact on the QoS parameters of a real-time application. It also introduces new QoS parameters at the connection and system levels. Currently, Mobile IP is based on the best effort delivery model and has no consideration of QoS. Furthermore, the RSVP model, which is efficient resource reservation in the fixed endpoints, becomes invalid under host mobility.

6.5.2 Integrated Services (Intserv)

The IETF set up an Integrated Services (Intserv) Working Group [24], which has defined several service classes that, if supported by the routers traversed by a data flow, can provide the data flow with certain QoS commitments. In the IntServ architecture, three classes of service is based on applications' delay requirements. These are the guaranteed-service class, which provides for delay-bounded service agreements; the controlled-load service class, which provides for a form of statistical delay service agreement (nominal mean delay) that will not be violated more often than in an unloaded network; and the well-known best-effort service, which is further partitioned into three categories: interactive burst (e.g., Web), interactive bulk (e.g., FTP) and asynchronous (e.g., e-mail). The main point is that the guaranteed service and controlled load classes are based on quantitative service requirements, and both require signalling and admission control in network nodes. These services can be provided either per-flow or per-flow-aggregate, depending on flow concentration at different points in the network. The level of QoS provided by these enhanced QoS classes is programmable on a per-flow basis according to requests from the end applications. These requests can be passed to the routers by network management procedures or, more commonly, using a reservation protocol such as RSVP, which is described in the third section. The requests dictate the level of resources (e.g., bandwidth, buffer space) that must be reserved along with the transmission scheduling behavior that must be installed in the routers to provide the desired end-to-end QoS commitment for the data flow. Although the IntServ architecture need not be tied to any particular signalling protocol, RSVP, is often regarded as the signalling protocol in IntServ. Best-effort service, on the other hand, does not require signalling.

The advantage of IntServ [21] is that it provides service classes, which closely match the different application types and their requirements. For example, the guaranteed service class is particularly well suited to the support of critical, intolerant applications. On the other hand, critical, tolerant applications and some adaptive applications can generally be efficiently supported by controlled load services. Other adaptive and elastic applications are accommodated in the best-effort service class. A major characteristic of IntServ it that it leaves the existing best-effort service class mostly unchanged except for a further subdivision of the class, so it does not involve any change to existing applications. This is an important property since IntServ is then capable of providing this class of service as efficiently as the current Internet. IntServ also leaves the forwarding mechanism in the network unchanged. This allows for an incremental deployment of the architecture, while allowing end systems that have not been upgraded to support IntServ to be able to receive data from any IntServ class with a possible loss of guarantee. End-to-end service guarantees cannot be supported unless all nodes along the route support IntServ. This is obviously so because any "pure" best-effort node along any route can treat packets in such a way that the end-to-end service agreements are violated. The subclassing of best-effort service, although already a significant improvement on the flat best-effort service currently provided in the Internet, may be considered somewhat "rough" in a commercial network.

6.5.3 Differentiated Services (Diffserv)

Differentiated services (Diffserv) [22] are a traffic handling mechanism and overcome the scalability concerns of RSVP. To provide QoS support, a network must somehow allow for controlled unfairness in the use of its resources. By recognizing the data flows generated by different applications can be ultimately classified into a few general traffic classes, the DiffServ architecture aims at providing simple and scalable service differentiation. It does this by providing a logical separation of the traffic in the different classes. It defines a field in packets' IP headers, called the diffserv codepoint (DSCP). Hosts or routers sending traffic into a diffserv network mark each transmitted packet with a DSCP value. Routers within the diffserv network use the DSCP to classify packets and apply specific queuing behavior known as *per-hop behavior* or PHB based on the results of the classification. Traffic from many flows having similar QoS requirements is marked with the same DSCP, thus aggregating the flows to a common queue or scheduling behavior. In both IPv4 and IPv6, the traffic class is denoted by use of the DS header field. The distinguishing feature of diffserv is its scalability. DiffServ is based on local service agreements at user/provider boundaries. Therefore, end-to-end services will be built by concatenating such local agreements at each domain boundary along the route to the final destination. The concatenation of local services to provide meaningful end-to-end services is an open research issue. The net result of the DiffServ approach is that per-flow state is avoided within the network, since individual flows are aggregated in classes.

To understand Diffserv's inherent scalability, it is important to contrast aggregate traffic handling mechanisms versus per-conversation traffic handling mechanisms. The traffic handling mechanisms envisioned in RSVP/Intserv networks are per-conversation mechanisms. These treat each traffic flow between each instance of a sending and receiving application, in isolation. Aggregate mechanisms, such as diffserv, group many traffic flows into a single aggregate class. Per-conversation traffic handling mechanisms rely on per-conversation classifiers. These typically use the IP source and destination addresses and ports to uniquely identify conversations. Aggregate traffic handling mechanisms typically rely on some mark in a packet that aggregates it into a queue shared by other packets with the same mark. Before the packet is submitted to the aggregate traffic handling mechanism, it must be marked with the appropriate tag. Aggregate traffic handling mechanisms require significantly less state and processing power in network nodes than their per-conversation counterparts. The compromise of aggregate traffic handling is that the QoS enjoyed by each conversation is dependent on the behaviour of the other conversations with which it is aggregated.

From the point of view of a flow, the class bandwidth is not a meaningful parameter. Indeed, bandwidth is a class property *shared* by all the flows in the class, and the bandwidth received by an individual flow depends on the number of competing flows in the class as well as the fairness of their respective responses to traffic conditions in the class. Therefore, to receive some quantitative bandwidth guarantees, a flow must reserve its share of bandwidth along the data path, which involves some form of end-to-end signalling and admission control at least among logical entities called *bandwidth broker*s. This end-to-end signalling should also track network dynamics i.e., route changes to enforce the guarantees. Furthermore, even qualitative bandwidth agreements require end-to-end signalling and admission control. This is because even if one class is guaranteed to have more bandwidth than another, the number and behaviour of flows in the latter class may result in smaller shares of bandwidth for these flows than for the flows in the other class. Hence, in this case, end-to-end signalling would also be required to ensure that in every node along the path, the bandwidth received by a flow in a high bandwidth class is greater than the bandwidth received by a flow in a smaller bandwidth class. On the other hand, delay and error rates are class properties that *apply* to every flow of a class. This is because in every router visited, all the packets sent in a given class share the queue devoted to that class. Consequently, as long as each router manages its queues to maintain a relative relationship between the delay and/or error rate of different classes, relative service agreements can be guaranteed without any signalling. However, if quantitative delay or error rate bounds are required, end-to-end signalling and admission control are also required.

The only functionality actually imposed by Differs in interior routers is packet classification. This classification is simplified from that in RSVP because it is based on a single IP header field containing the DSCP, rather than multiple fields from different headers. This has the potential of allowing functions performed on every packet, such as traffic policing or shaping, to be done at the boundaries of domains, so forwarding is the main operation performed within the provider network. Another advantage of DiffServ is that the classification of the traffic, and the subsequent selection of a DSCP for the packets, need not be performed in the end systems. Indeed, any router in the stub network where the host resides, or the ingress router at the boundary between the stub and provider networks, can be configured to classify on a per-flow basis, mark, and shape the traffic from the hosts. Such routers are the only points where per-flow classification may occur, which does not pose any problem because they are at the edge of the Internet, where flow concentration is low. The potential non-involvement of end systems, and the use of existing and widespread management tools and protocols allow swift and incremental deployment of the DiffServ architecture.

A hierarchical model for network resource management is used to achieve the scalability and flexibility in DiffServ. This model contains Interdomain and Intradomian resource management:

- Interdomain resource management provides unidirectional service levels and traffic contracts that are agreed at each boundary point between a user and a provider for the traffic entering the provider network.
- Intradomain resource management facilitates the service provider who is doing the configuration and provisioning of resources within its domain i.e., the network.

The different service providers build their offered services with a combination of traffic classes to provide controlled unfairness at their boundaries. Traffic conditioning a function that modifies traffic characteristics to make it conform to a traffic profile and thus ensure that traffic contracts are respected, and billing to control and balance service demand. For example, traffic conditioning i.e., metering, marking, shaping, or dropping in the interior of a network is left to the discretion of the service providers. Provisioning and partitioning of both boundary and interior resources are the responsibility of the service provider. For example, DiffServ does not impose either the number of traffic classes or their characteristics on a service provider. Although interior routers nominally support traffic classes, DiffServ does not impose any requirement on interior resources and functionalities.

Simultaneously providing several services with differing qualities within the same network at the same time is rather new area. Despite its apparent simplicity, DiffServ does not make this task any simpler. Instead, in DiffServ it was decided to keep the operating mode of the network simple by pushing as much complexity as possible onto network provisioning and configuration. Unless resources are massively over provisioned in both interior and border routers, traffic and network dynamics can cause momentary violation of service agreements, especially those relating to quantitative services. In such a case, the service would apply only to packets entering the domain at a designated ingress router and leaving the domain at a designated egress router. The egress router is in the route to any given destination, the interdomain routing entry for that destination must be statically fixed in the ingress router. Even for a fixed ingress-egress pair, intradomain routing dynamics can still occur. This means that the set of internal routers visited by the packets travelling between the ingress and egress routers can still suddenly change. However, the "directionality" of the traffic considered here is such that the number of possible routes is considerably reduced compared with the general case, and so is the resulting and necessary over provisioning. A service provider could, however, reduce to a minimum the over provisioning of quantitative services offered between pairs of border routers by "pinning" the intradomain route between those routers. Fixing the egress router for a given destination and/or pinning internal routes between border routers nevertheless incur a loss of robustness. In multicast, where receivers can join and leave the communication at any time, the problem of efficient provisioning will be even worse. Alternatively, a service provider might wish to use dynamic logical provisioning and configuration i.e., sharing of resources between classes as an answer to the problems of network and traffic dynamics. However, depending on the type of service agreement qualitative, relative, or quantitative and the QoS parameters involved in the agreement, dynamic logical provisioning might require signalling and admission control. End-to-end signalling and admission control would increase the complexity of the DiffServ architecture.

6.5.4 Resource Reservation Protocol (RSVP)

The Resource Reservation Protocol (RSVP) is developed on the concept of the communication session [25]. To support different services [26], it is designed to enable the senders, receivers, and routers of either multicast or unicast communication sessions to communicate with each other in order to set up the necessary router state. This communication session is composed of at least one data flow to a destination by a combination of the triplet: destination address, destination port, and protocol id. As RSVP is not a routing protocol, it is used to reserve resources along the existing route set up by whichever underlying routing protocol is in place. RSVP as a receiver-driven protocol scales to large numbers of participants in multicast groups. The reservation request from a receiver does not have to propagate all the way to the sender in most situations. If the reservation request encounters an existing reservation in one of the RSVP routers along the route, which is equal to or greater than its own reservation and does not travel any further. This also allows for incremental reservations whereby some receivers behind a bottleneck can hold partial reservations and then regularly poll the network, hoping for completion of full reservations. Figure 6.9 shows an example of RSVP for a multicast session involving one sender, S1, and three receivers, RCV1–RCV3.Path messages are periodically sent toward the destination and establish a path per flow in the routers. A flow is defined as any subset of the packets in a session i.e., as a subset of the packets sent to a given destination. Resv messages are periodically sent toward the sources, and establish the required reservations along the path followed by the data packets. In order to reduce the overhead associated with RSVP, that router does not forward any Path or Resv message that does change the states held by a router immediately. Instead, each router periodically issues its own Path and Resv messages carrying information about the flows it holds. A lifetime is associated with each reserved resource. This timer is reset each time a Resv message confirms the use of the resource. If the timer expires, the resource is freed. This principle of resource management based on timers is called soft state. Soft state is also applied to the path state in the routers in this case; the timer is reset upon reception of a Path message.

The soft state mechanism is a very simple self-stabilizing mechanism to keep the nodes of the network in a consistent state. It provides natural recovery form node crashes, as well as preventing resource leaks by reclaiming resources made obsolete by various conditions e.g., route changes, loss of teardown messages, users leaving a multicast group without explicitly releasing resources. Teardown messages (PathTear and ResvTear) are available for immediate release of the corresponding states (path and reservations). The sender or receiver, or any intermediate RSVP router upon state timeout or service preemption can initiate teardown requests. The concept of acknowledgment is not used in RSVP; all the messages are delivered unreliably because of the protocol reliance on soft states. RSVP has also been designed to operate across non-RSVP networks. It is difficult to guarantee the end-to-end service in such a case. This allows for a progressive deployment of the protocol associated with an improvement of the end-to-end best-effort service seen by flows exploiting RSVP in the part of the Internet where it is supported.

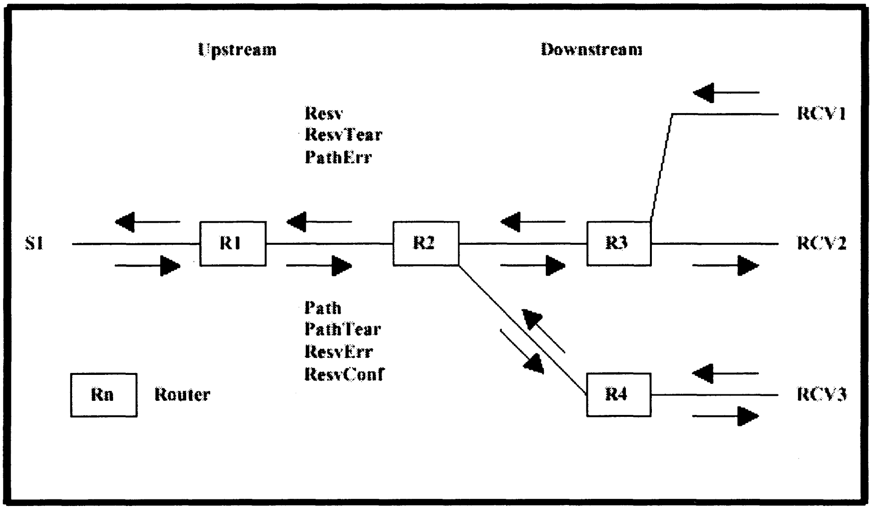


Figure 6.9 RSVP Messages

A new mechanism called local repair has been used to improve the RSVP responsiveness to network dynamics. When an RSVP entity detects a change of route, it sends Path messages down the new route for the flows whose route has changed. When the downstream RSVP entity, situated at the junction of the old and new routes, receives these Path messages, it updates its path states accordingly and immediately sends a Resv message upstream along the new segment of the route for the corresponding flows. Local repairs take care of establishing resources on new portions of a route after a route change. However, these cannot be relied on across a non-RSVP cloud, because an RSVP node located just before the non-RSVP area may not detect routing changes that affect the egress path from such a cloud.

Therefore, soft state (and its associated periodic messages) also provides an easy solution to route changes in non-RSVP areas of the network.

RSVP allows several styles of reservation: distinct resources may be assigned to given flows, while several flows may share some resources. A flow for which no resource has been reserved gets best-effort service from the routers. The different reservation styles improve resource usage efficiency in the nodes of the network. For instance, shared reservations are well suited to scenarios where multiple sources are unlikely to transmit simultaneously (e.g., audio sources in conferencing applications), because, in such a case, the size of the shared reservation is essentially independent of the number of sources. It should be noted that shared reservations provide for an overall gain in reservation efficiency. In RSVP's current specification stage, it does not influence the routing of packets, which are therefore routed by IPv4 or IPv6.

In the wireless mobile networks, RSVP must re-establish [27] reservations along the new path from the mobile node (MN), which is a receiver and moves to another location, to the source. In general, each source initiates Path messages periodically to reserve resources along a new path after the change of routing happens. The mobile node has to wait for a Path messages at its new visited location before it can send a Resv message back for reservation of resources along the new path to the source. Whenever MN moves one location to another location, then it occurs a path change and the new path to the MN from the correspondent node (CN) is found out by RSVP after expiring the soft state in routers. This mechanism leads to large delays under a roaming environment with the mobility of host. The new mechanisms are devised to reduce the reservation delay for resource and packet loss originating from handoffs under RSVP.

6.5.5 RSVP Extensions

The micromobility [28] is the mobility across different cells under same the subnet while the macromobility is the mobility from one subnet to another subnet. The RSVP is mainly considered with Mobile IP under macromobility, but routers or intermediate nodes under micromobility are RSVP-enabled to provide QoS guarantee for mobile users using real-time applications. An approach involves changing the RSVP implementation at the routers to which BSs are connected. In this scheme, whenever the MN moves into the neighbouring cell, resource reservations are made newly over a two-hop link between the router/intermediate nodes and the MN. Once the BS detects the MN's handoff, it notifies router/intermediate nodes, and thus Path and Resv messages are exchanged to make a new reservation between the router/intermediate nodes and the MN. Therefore, the resource reservations delay over only a two-hop link will be very short, and guaranteed QoS in the newly modified portion of the path can be obtained easily. For more general approaches under micromobility including various topologies (e.g., Cellular IP), a new path needs to be set up during a handover. In setting up a new path, the remaining circuits need to be reused because only a partial path is changed. This kind of path reestablishment scheme requires discovery and setup of the new partial path between the crossover router/intermediate nodes and the MN during handoff. While the signalling overhead depends on the connection setup protocol, the number of hops required to set up the partial path during a handover is crossover-router/intermediate nodes-dependent; end-to-end latency is a function of the route length. Hence, an efficient partial path discovery mechanism is required so that the RSVP resource reservation delay is reduced, resulting in being able to get guaranteed QoS for real-time services.

An inter-subnet handoff occurs when the MN moves to another BS that is connected to another router. In Mobile IP, an MN registers with its HA each time it changes its point of attachment. When the HA is distant from the MN, the delay to complete an update could be significantly high. Mobile IP has been optimised for macromobility and relatively slow-moving mobile hosts. It causes disruption during handoff, and high signalling overhead due to frequent notification to the MN's HA. Therefore, Mobile IP does not scale well to serve a large number of mobile users moving frequently between small cells. There have been several protocols on RSVP supporting macromobility.

6.5.5.1 RSVP Tunnel with Mobile IPv4

This protocol is a simple QoS signalling protocol by combining preprovisioned RSVP tunnels with Mobile IPv4 and the figure shows the RSVP tunnel model with Mobile IP when an MN is a receiver. When the MN moves to cell B, it informs its home agent of its new location. When the HA is informed about the MN's new location, it does two activities: First, it sets up a tunnel RSVP session between itself and the foreign agent (FA) if one does not exist between them and second: it encapsulates Path messages from the sender and sends them through the tunnel toward the MN's new location. When the FA receives a Resv message from the visiting mobile node, it sends a Resv message for the corresponding tunnel session between itself and the HA. After sending the reservation request, the FA waits for a confirmation from the HA that the reservation over the tunnel was successful. This approach can easily be implemented with minimal changes to other components of the Internet architecture. However, when a mobile host roams far away from the HA, the triangle routing problem occurs, but there is no consideration of the shortest path mechanism such as route optimization. In this protocol, there is also no solution for reducing service disruption due to frequent mobility of a host.

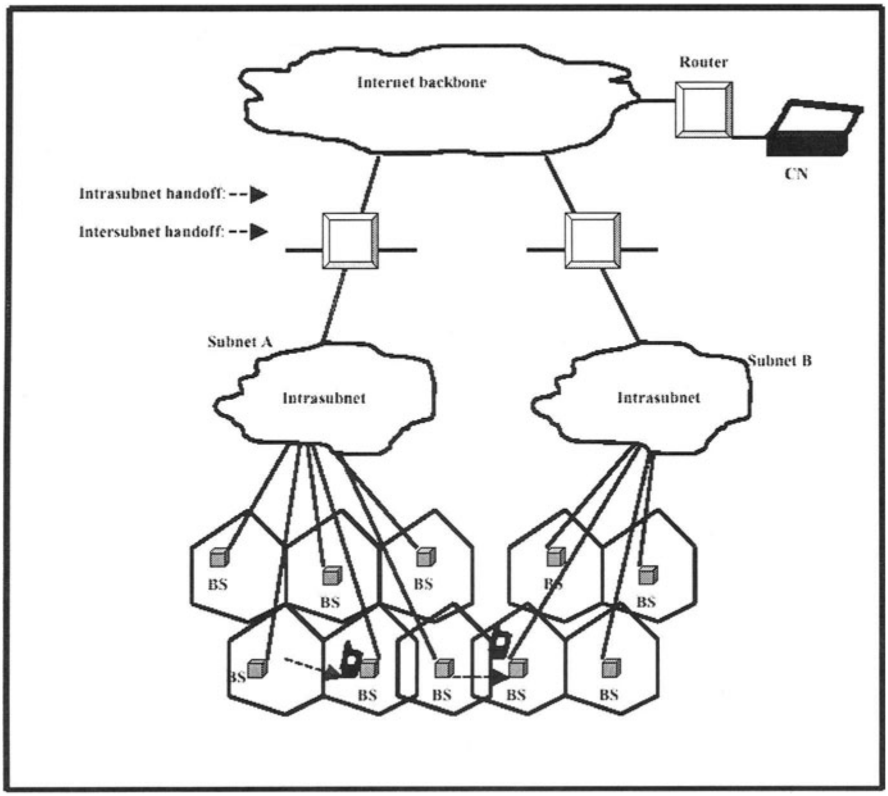


Figure 6.10 Handoffs in Micro- and Macro-mobility domains

6.5.5.2 Mobile IPv6 and RSVP Integration Model

This protocol [29] is an integration model of Mobile IPv6 and RSVP and the Figure 6.11 shows this integration model of Mobile IPv6 and RSVP when MN is a receiver. The main idea of this integration of protocols is that they will use RSVP to reserve resources along the direct path between the CN and the MN without accessing their HAs because Mobile IPv6 has route optimization facility.

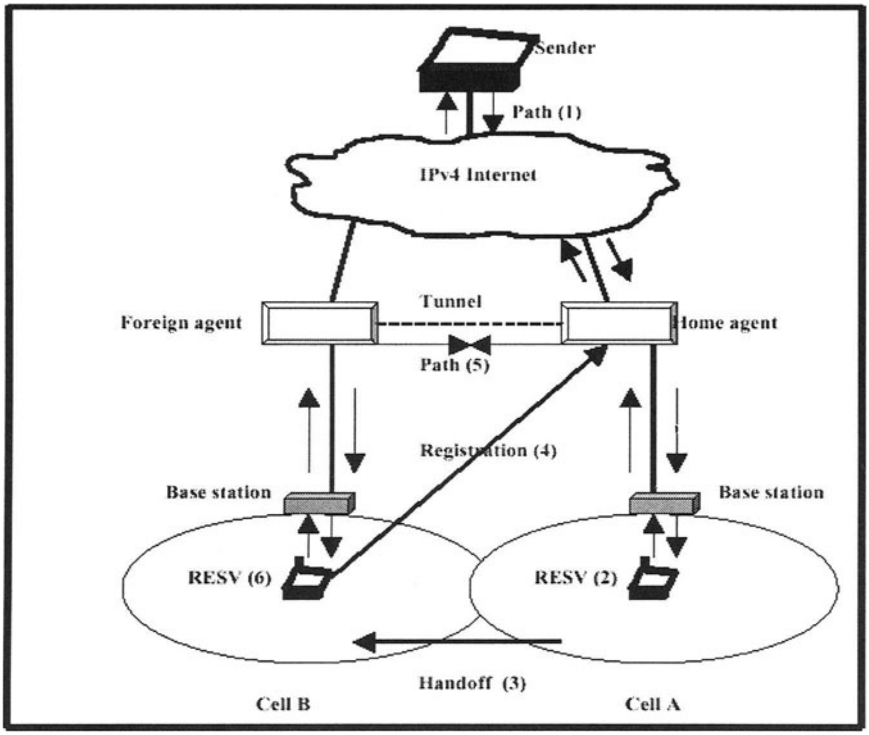


Figure 6.11 RSVP Tunnel with Mobile IPv4

In this model, resources are initially reserved between the CN and the MN's original location. Whenever the MN performs a handoff, which incurs a path change, a new RSVP signalling process is invoked immediately to reserve resources along the new path. When the MN performs a handoff from subnet A to subnet B, it gets a new CoA and subsequently sends a binding update to the CN. The CN then sends a Path message associated with the new flow from CN to MN. Upon receiving this Path message, the MN replies with a Resv message immediately to reserve resources for the new flow. For each handoff, the MN as receiver has to wait for a new Path message from the CN; only after getting the Path message can it issue a new Resv message to the CN. However, all these RSVP renegotiations are conducted end to end even though the path change may only affect a few routers within the whole path during a single handoff. Hence, the long handoff resource reservation delays and large signalling overheads caused by this end-to-end RSVP renegotiation process could lead to notable service degradation in providing real-time services. Furthermore, during this period there might not be enough resources in the newly added portion of the flow path between CN and MN.

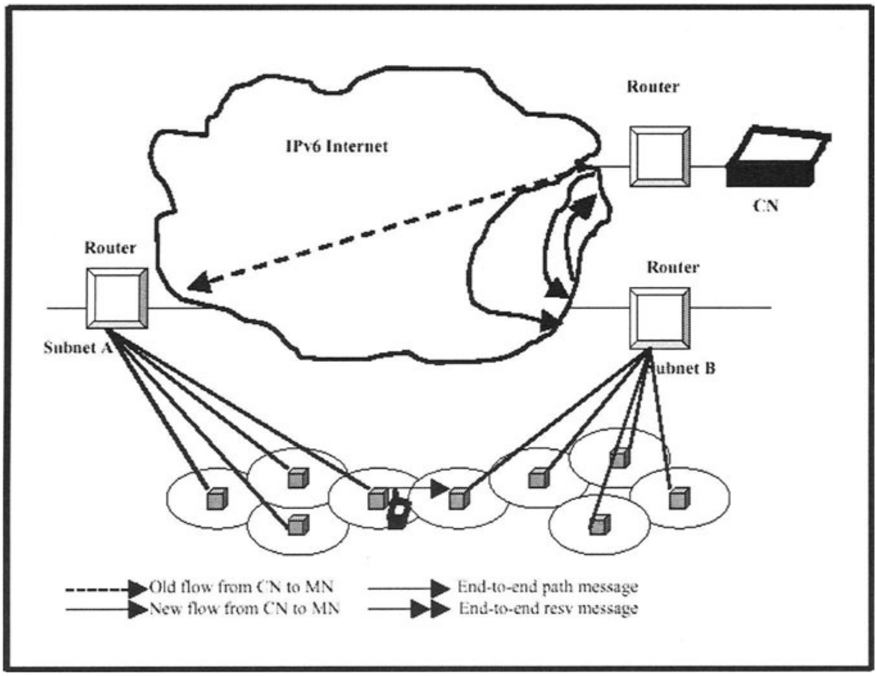


Figure 6.12 Mobile IPv6 and RSVP integration model

6.5.5.3 Mobile IP with Location Registers

This protocol called MIP-LR (Mobile IP with Location Registers) [30] is more suitable for 3G cellular systems. This scheme uses a set of databases, called location registers, to maintain the current CoA of the mobile host. When an MN moves from one subnet to another, it registers its current CoA with a database called a home location register (HLR). When a CN has a packet to send, it first queries the HLR to obtain the mobile host's CoA, and then sends packets directly to the mobile host; the CN caches the MN's CoA to avoid querying the HLR for every subsequent packet destined for the MN. MIP-LR not only eliminates the inefficiency of triangle routing in MIP, but also generally avoids tunnelling and allows resource reservation using RSVP to provide QoS guarantees.

6.5.5.4 Mobility Support based on Flow Transparency

This protocol [31] proposed a method to solve the drawbacks in the existing IPv6 QoS with mobility support model, namely, long resource reservation delays and large signalling overheads. In this model, the RSVP session and flow identity at the network level should be constantly unique for the flow handling mechanism (e.g., the packet classifier) in the router regardless of node mobility. When the MN is acting as a receiver, instead of the CN, the crossover router (CR) issues a Path message to the mobile receiver because the required information already exists in the CR during the previous RSVP message exchanges. In order to detect the route change of the receiver and trigger local repair for the receiver, the receiver should be able to inform the CR of its handoff information, which contains the flow destination and the MN's current address. This method automatically limits the handoff RSVP renegotiation process within the newly added portion of the path between CN and MN. Therefore, handoff resource reservation delays and signalling overheads can be minimized, which in turn minimizes the handoff service degradation. However, when the MN is acting as a sender, current Mobile IPv6 sets the source address (of packets originated from an MN) to the MN's CoA, and the MN's home address is moved into a home address option in a destination options header, which is not processed by intermediate routers during packet transmission. Only changing the flow source to be the MN's home address causes a problem for router packet classification. Hence, implementation of this model requires some modification to Mobile IPv6. There is also no mechanism to guarantee the same level of resources in a new point of attachment to which the mobile host moves. This may cause service disruption with mobility of the host.

6.6 MULTIPROTOCOL LABEL SWITCHING (MPLS)

6.6.1 Background and Structure

Multiprotocol label switching (MPLS) is the convergence of connection-oriented forwarding techniques and the Internet's routing protocols [32] [33]. The term *multilayer routing* covers approaches to the integration of layer 3 datagram forwarding and layer 2 switching that go beyond the use of the techniques found within gigabit routing/switching. The approach uses label lookups to allow more efficient packet classification, and the potential to engineer the network and manage the impact of data flows. By adding new capabilities to the IP architecture, MPLS enables support of new features and applications. The new applications include traffic engineering [34] [35], IP virtual private networks [36], integration of IP routing and layer 2 or optical switching [37], IP QoS and other applications. The most prominent pre-standard incarnations of MPLS leveraged the high-performance cell switching capabilities of asynchronous transfer mode (ATM) switch hardware, and melded them together into a network using existing IP routing protocols [38]. As standardization progressed, packet-based MPLS also emerged to simplify the mechanics of packet processing within core routers. The role of MPLS is the Internet's best long-term solution to efficient, high performance forwarding and traffic differentiation (IP QoS). However, an important consideration is that there is much in common between the technology of MPLS networks and IP routed networks. The overlap in technology means that there is much in common between the process of design of MPLS networks and the design of other IP routed networks.

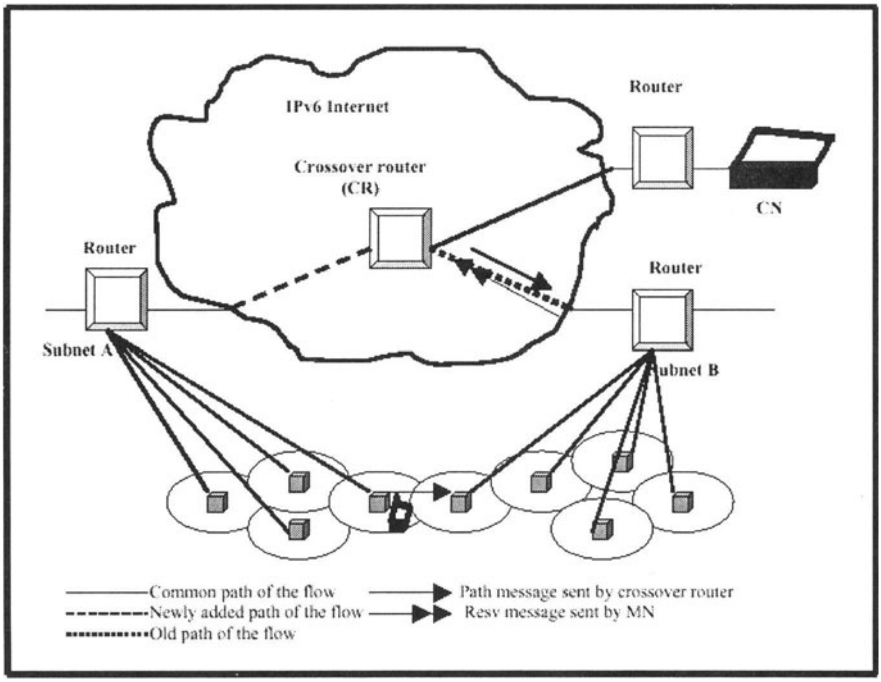


Figure 6.13 Mobility support based on flow transparency

The earliest motivation for developing MPLS lay in the desire to simplify wide-area, high-performance IP backbone architectures. In theory, an IP/ATM network consisted of logical IP subnets (LISs) interconnected by routers [34]. Inter-LIS traffic traveled through routers even when a direct ATM path existed from source to destination. This single LIS approach has two scaling problems: the number of virtual channels (VCs), and the number of interior gateway protocol (IGP) peers. In practice, a single LIS backbone would result in each router having a VC open to every other router to build up a mesh. A mesh of IGP peering relationships would also be created among the routers in the LIS. Adding each new router became an ATM-level problem too, since the *(N*+ 1)th router resulted in *N* new VCs being added across the ATM network. MPLS solves the IP/ATM scaling problem by making every interior ATM switch an IGP peer with its neighbors (other directly attached ATM switches or the directly attached IP Routers originally "surrounding" the single LIS). ATM switches become IGP peers by having their ATM control plane replaced with an IP control plane running an instance of the network's IGP. With the addition of the Label Distribution Protocol (LDP) [35], each ATM switch becomes a core (or interior) LSR, while each participating IP router becomes an edge LSR (or label edge router, LER). Core LSRs provide transit service in the middle of the network, and edge LSRs provide the interface between external networks and the internal ATM switched paths. The demands on the IGP drop dramatically, since each node now has only as many peers as directly ATM-attached neighbours.

An MPLS network such as that in Figure 6.14 consists of edge label switch routers (edge LSRs) around a core of label switch routers (LSRs). Customer sites are connected to the carrier's MPLS network, or equivalently a large organization's network backbone. Figure 6.14 shows nine customer sites and four edge LSRs, but more typically there will be hundreds or more customer sites per edge LSR. The customer premises equipment connected to an MPLS network typically runs ordinary IP forwarding rather than MPLS, and is typically a router or a LAN switch. Since the customer equipment typically does not run MPLS, the edge LSRs are part of the carrier's network and under the carrier's administration. A carrier's MPLS network will often be connected to one or more other IP networks as part of the Internet. An IP connection to another carrier might be an MPLS link, although use of MPLS on intercarrier links is usually not required. As with any interconnection of carrier networks in the Internet, the Border Gateway Protocol would typically operate over links to other carriers, to exchange routing information with them. The neighboring IP networks may use MPLS internally, but not necessarily. The links between customer equipment, edge LSRs, and/or LSRs may be of virtually any type.

Many packets follow much the same shortest paths across any given IP backbone regardless of their final destination(s). The MPLS Working Group gives the name *forwarding equivalence class* (FEC) to each set of packet flows with common cross-core forwarding path requirements. LDP dynamically establishes a shortest path VC (now known as a label-switched path, or LSP) tree between all the edge LSRs for each identifiable FEC. The label —virtual path/channel identifier (VPI/VCI) — at each hop is a local key representing the next-hop and QoS requirements for packets belonging to each FEC. VC utilization is no worse than the single LIS case, and with the introduction of VC-merge-capable ATM-based LSRs it can be much more efficient (only a single VPI/VCI is required downstream of the merge point, regardless of the number of VCs coming in from upstream). Pure packet-based MPLS networks are a trivial generalization of the ATM model; simply replace the ATM- based core LSRs with IP router-based core LSRs, and use suitable packet-based transport technologies to link the LSRs.

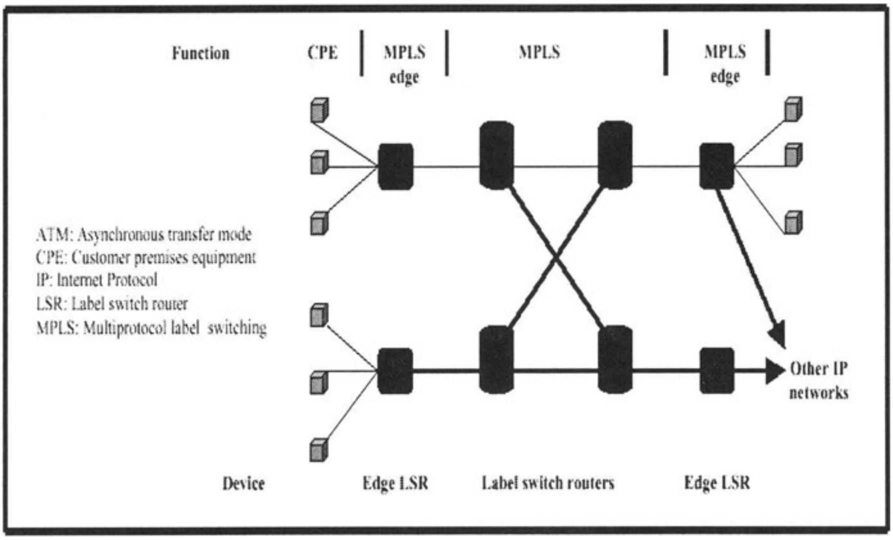


Figure 6.14 MPLS network architecture

Each MPLS packet has a header that is either encapsulated between the link layer and the network layer, or resides within an existing header, such as the virtual path/channel identifier (VPI/VCI) pair within asynchronous transfer mode (ATM). At most, the MPLS header will contain a label, TTL field, Class of Service (CoS) field, stack indicator, next header type indicator, and checksum.

MPLS packets are able to carry a number of labels, organized in a last-in first-out stack. This can be useful in a number of instances, such as where two levels of routing are taking place across transit routing domains. Regardless of the existence of the hierarchy, in all instances the forwarding of a packet is based on the label at the top of the stack. In order for a packet to travel through a tunnel, the node at the transmitting side of the tunnel pushes a label relating to the tunnel onto the stack, and sends the packet to the next hop in the tunnel. A collection of LSRs goes together to make a *label-switched path* (LSP). Two options are defined for the selection of a route for a particular forwarding class. Hop-by-hop routing defines a process where each node independently decides the next hop of the route. Explicit routing is where a single node (often the ingress node of a path) specifies the route to be taken (in terms of several or all of the LSRs in the path). Explicit routing may be used to implement network policies, or allow traffic engineering in order to balance the traffic load.

There are two approaches to label path control. Independent path control means that LSRs are able to create label bindings and distribute these bindings to their peers independently. This is useful when bindings relate to information distributed by routing protocols, and means that nodes can begin to label switch before the completion of a path. Ordered path control means label binding only takes place if the node is the egress node for the particular FEC, or has received a label binding for that FEC from its next hop. This approach is used to ensure that a particular traffic class follows a path with a specified set of QoS properties.

6.6.2 Traffic and QoS Properties

There are three main approaches [21] for identifying traffic to be switched. First, path creation can be control-driven or topology-driven, where labels are preassigned in relation to normal routing control traffic. Here, the network size dictates the load and bandwidth consumed by the assignment and distribution of label information. Second, request-based control traffic from protocols such as RSVP can trigger path creation relating to individual flows or traffic trunks. Here, the number of labels and computational overhead will depend entirely on the number of flows being supported. Finally, data-traffic-driven label assignment is where the arrival of data recognized as a flow activates label assignment and distribution on the fly. This approach implies that there will be latency while path setup takes place. Overheads in this case will be directly proportional to traffic patterns.

MPLS is able to work in an environment that uses any data link technology, connection-oriented and connectionless. MPLS also provides the potential for all traffic to be switched, but this depends on the granularity of label assignment, which again is flexible and depends on the approach used to identify traffic (discussed above). Labels may be assigned per address prefix (e.g., a destination network address prefix) or set of pre-fixes, and can also represent explicit routes. On a finer-grained level, labels can be defined per host route and also per user.

At the lowest level, a label can represent a combined source and destination pair, and in the context of RSVP can also represent packets matching a particular filter specification. MPLS needs a mechanism for distributing labels in order to set up paths. The architecture does not assume that there will be a single protocol LDP to complete this task, but rather a number of approaches that can be selected depending on the required characteristics of the LSPs. Where paths relate to certain routes, label distribution could be piggybacked onto routing protocols. Where labels are allocated to the packets of a specific flow, distribution can be included as part of the reservation protocol. New protocols have been developed for general label distribution and the support of explicitly routed paths. MPLS label distribution requires reliability and the sequencing of messages that relate to a single FEC. While some approaches use protocols that sit directly over IP (thus implying they are unlikely to be able to meet these reliability requirements), a number of the defined LDPs solve this issue by operating over TCP.

Within the MPLS architecture, label distribution binding decisions are generally made by the downstream node, which then distributes the bindings in the upstream direction. This implies that the receiving node allocates the label. However, there are also instances (especially when considering multicast communications) where upstream allocation may also be useful. In terms of the approach to state maintenance used within MPLS, a soft state mechanism is employed, implying that labels will require refreshing in order to avoid timeouts. Approaches to this include the MPLS peer keep-alive mechanism, and the timeout mechanisms inherent within routing and reservation protocols (in instances where they are used to carry out label distribution). In terms of support for QoS, MPLS provides the CoS field which enables different service classes to be offered for individual labels. For more fine-grained QoS provisioning, the CoS field could be ignored, using a separate label for each class. In this instance, the label would represent both the forwarding and service classes. As noted earlier, MPLS is able to provide QoS support on a per-flow basis using either flow detection or request-based control traffic from protocols such as RSVP to trigger label assignment. More general QoS differentiation can be achieved by such means as label assignment on a per-user basis, and using more general traffic engineering techniques.

6.7 IP OVER WDM

Now we discuss possible techniques suggested in the literature to explore the potential of putting IP directly on top of WDM.

6.7.1 IP and WDM Integration

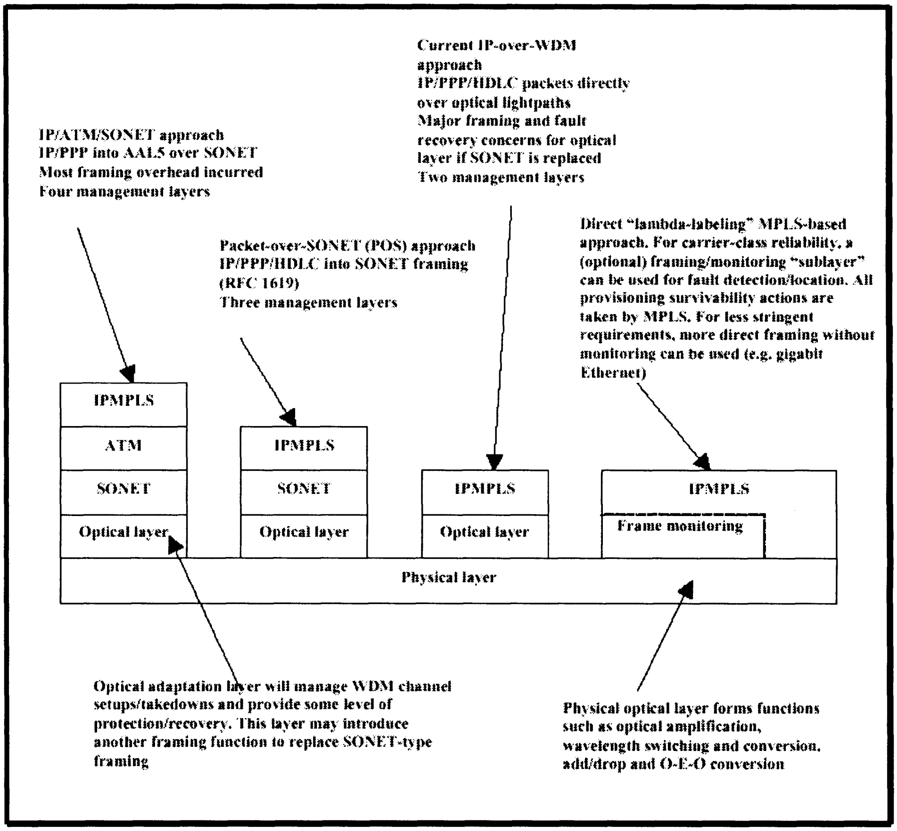
Along with the emergence of today's Internet and its related applications, based on IP, the development of wavelength-division multiplexed (WDM) techniques on point-to-point links has utilized the optical bandwidth of available optical fibres [32]. The *IP over WDM integration* encompasses a wide range of solutions to supporting predominantly IP traffic over WDM optical paths.

Currently, most IP transport architectures are based on synchronous optical network/synchronous digital hierarchy (SONET/SDH), encapsulating IP packets (or ATM cells carrying IP packets) in SONET/SDH frames. The future deployment of optical cross-connected WDM transport networks, managing optical light paths dynamically in multiple ring or mesh architectures, will potentially modify the role of the network functionalities provided by the SONET/SDH layer. Toward this end, a key advantage of WDM is that it offers multiprotocol support, allowing multiple, and independent network protocols to coexist on the same fibre network. However, this full-stack approach reduces efficiency and poses increased management/operation costs, given in Figure 6.15. Therefore, designing a single, ubiquitous WDM (optical) access layer with tight IP interworking can significantly reduce the intermediate layering requirements i.e., the *IP-MPLS/optical layer.*

In order to provision a full range of network functionality, the optical layer must subsume some key functions, which currently reside in different network layers. These include channel routing, channel monitoring, and fault detection and recovery capabilities. Furthermore, other approaches based on the IP MPLS framework, such as *lambda labeling* and *multiprotocol lambda switching*, have also been proposed to subsume optical-layer provisioning functionality within the IP domain, allowing for even closer IP-WDM layer integration.

The early deployment of WDM technology as a point-to-point solution for capacity exhaustion has helped shift the speed bottleneck from link bandwidth to higher-layer electronic nodes, such as IP routers and ATM switches. The lack of optical processing capabilities results in increased *opto-electronic-optic* (O-E-O) conversion requirements, which in turn lead to reduced processing speeds and scalability concerns.

As an alternative solution, WDM subsystems can be used to switch individual wavelengths optically and establish cut-through *lightpaths*, also known as *channels*, between non-adjacent nodes, thereby bypassing intermediate protocol processing. This allows for overlaying virtual higher-layer protocol topologies on top of the physical fibre topology, where the light-paths represent virtual links. Wavelength routing improves the connectivity between electronic network-layer nodes (equipped with tunable WDM laser interfaces), thereby simplifying higher-layer routing and reducing the net processing overhead per unit of transmitted data.



IP/ATM/SONET approach
IP/PPP into AAL5 over SONET
Most framing overhead incurred
Four management layers

Packet-over-SONET (POS) approach
IP/PPP/HDLC into SONET framing
(RFC 1619)
Three management layers

Current IP-over-WDM
approach
IP/PPP/HDLC packets directly
over optical lightpaths
Major framing and fault
recovery concerns for optical
layer if SONET is replaced
Two management layers

Direct "lambda-labeling" MPLS-based approach. For carrier-class reliability, a (optional) framing/monitoring "sublayer" can be used for fault detection/location. All provisioning survivability actions are taken by MPLS. For less stringent requirements, more direct framing without monitoring can be used (e.g. gigabit Ethernet)

Optical adaptation layer will manage WDM channel setups/takedowns and provide some level of protection/recovery. This layer may introduce another framing function to replace SONET-type framing

Physical optical layer forms functions such as optical amplification, wavelength switching and conversion, add/drop and O-E-O conversion

Figure 6.15 Protocol stack developments for IP over WDM Integration

6.7.2 IP over Optical Network Architectures

To examine the architectural alternatives for IP over optical networks, IP routers at the edge of the optical networks must establish lightpaths before the communication at the IP layer can begin [40]. Thus, the IP data plane over optical networks is realized over an overlay network of lightpaths. On the other hand, IP routers and optical cross-connects (OXCs) can have a peer relation on the control plane, especially for implementation of a routing protocol that allows dynamic discovery of IP endpoints attached to the optical network. The IP-over-optical-network architecture is defined essentially by the organization of the control plane. Clearly, there is a strong need to improve the protocol interface between the lower WDM optical layer and the higher electronic network layers. Additionally, interface definitions between optical networks themselves are also required to extend optical services over larger domains that are given in Figure 6.15. Most current works are focused on developing a ubiquitous WDM *adaptation* protocol-layer entity to provision lightpath circuit services to various client layer protocols, for example, the *optical user–network interface* (O-UNI) concept. This is expected to be part of a larger multivendor interoperable *operations, administration, and maintenance* (OAM) framework for optical networks. The main functions here include channel provisioning, fault management, and service monitoring. Although proprietary WDM adaptation solutions are available, significant standardization issues remain before multivendor interoperable protocols emerge.

The control plane based on IP routing protocols and MPLS signalling protocols is used in the optical network. Depending on the service model, however, the control planes in the IP and optical networks can be loosely or tightly coupled. This coupling determines:

- The details of the topology and routing information advertised by the optical network across the user-network interface (UNI)
- The level of control IP routers can exercise in selecting specific paths for connections across the optical network

The following interconnection models are possible for IP over optical networks [2].

- *The peer model*: Under this model, the IP and optical networks are treated together as a single integrated network managed and traffic engineered in a unified manner. In this regard, the OXCs are treated just like any other router as far as the control plane is concerned. Thus, from a routing and signalling point of view, there is no distinction between the UNI, the network-network interface (NNI), and any other router-to-router interface. A single routing protocol instance runs over both the IP and optical domains. The advantage of the peer model is that it allows seamless interconnection of IP and optical networks; its drawback is that it requires routing information specific to optical networks to be known to routers.

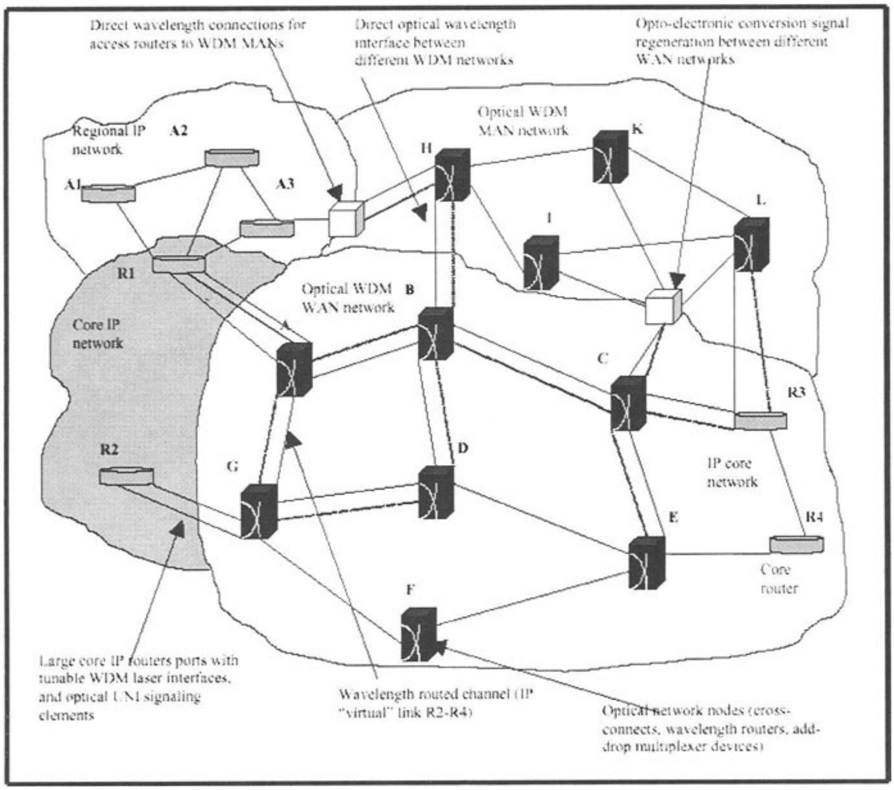

Direct wavelength connections for access routers to WDM MANs
Direct optical wavelength interface between different WDM networks
Opto-electronic conversion signal regeneration between different WAN networks
Regional IP network
A2
A1
A3
Optical WDM MAN network
H
K
I
L
R1
Core IP network
Optical WDM WAN network
B
A
C
R3
R2
G
D
IP core network
E
R4
Core router
F
Large core IP routers ports with tunable WDM laser interfaces, and optical UNI signaling elements
Wavelength routed channel (IP "virtual" link R2-R4)
Optical network nodes (cross-connects, wavelength routers, add-drop multiplexer devices)

Figure 6.16 Optical Mesh Transport Network

- *The overlay mode*l: Under this model, the IP network routing, topology distribution, and signalling protocols are independent of the corresponding protocols in the optical network. This model is conceptually similar to classical IP over ATM, but applied to an optical subnetwork directly. The advantage of the overlay model is that it is the most practical for near-term deployment; its drawback is that it requires the creation and management of IP routing adjacencies over the optical network.
- *The interdomain mode*l: Under this model, there are actually separate routing instances in the IP and optical domains, but information from one routing instance is passed through the other routing instance. For example, external IP addresses could be carried by the optical routing protocols to allow reachability information to be passed to IP clients. The interdomain model combines the best of the peer and overlay interconnection models; it

is relatively easy to deploy compared to the peer model in the near term, but does not require the management of IP routing adjacencies over the optical network.

To generalize lightpath services provisioning, it is desirable for the adaptation protocol to define a complete set of channel features [7]. This set comprises but is not necessarily limited to pertinent channel attributes such as bandwidth (i.e., granularity), quality, policy /priority, and survivability. These features are specified in channel requests, and subsequently incorporated into the optical routing and survivability provisioning algorithms. For example, it is well known that physical-layer effects are much more pronounced in optical networks than in electronic networks (i.e., power loss, crosstalk, dispersion, noise amplification, and other nonlinearities) [1, 2, 6]. Hence, the quality attribute can specify various requirements relating to a QoS such as light-path bandwidth, delay, and bit error rate (BER). Route provisioning algorithms would incorporate these attributes to ensure that channel qualities are met. Meanwhile, the policy/priority attribute can incorporate other higher-level requirements into the routing/survivability strategies in addition to the regular resource utilization constraints [7]. Such a feature could be used to control channel set-ups by an offline virtual topology control application/protocol. Similarly, the survivability attribute can define various types and levels of channel protection and restoration desired, as discussed in the next section.

6.7.3 IP-Centric Control: Provisioning and Restoration

Provisioning and restoring lightpaths end-to-end between IP networks requires protocol and signalling support within optical subnetworks and across the optical NNI. We consider the problem of controlling provisioning and restoration within a single optical subnetwork [40].

The topology of a single optical subnetwork is illustrated in Figure 6.17. The neighbouring OXCs may have multiple links between them. Each OXC is capable of switching a data stream from a given input port to a given output port. This switching function is controlled by appropriately configuring a cross-connect table. A lightpath from an ingress port in an OXC to an egress port in a remote OXC is established by setting up suitable cross-connects in the ingress and egress, and a set of intermediate OXCs such that a continuous physical path exists from the ingress to the egress port. Light-paths are assumed to be bi-directional: the return path from the egress port to the ingress port follows the same route as the forward path.

The following mechanisms are required to support automated provisioning of lightpaths within a subnetwork:

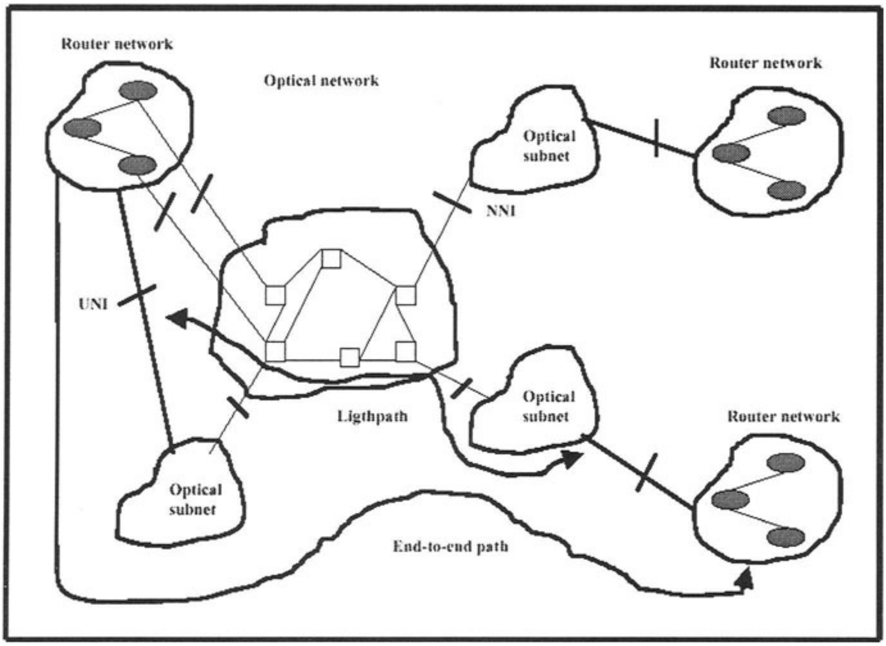


Figure 6.17 IP-over Network Model

- Neighbour discovery: Automatic detection of links between neighbouring OXCs and keeping track of their status (e.g., up/down, bandwidth availability)
- Link state update: Collecting the link state information from each OXC to determine the current topology and link state characteristics of the entire subnetwork
- Route computation: Computation of a route for the lightpath being set up, taking into account the bandwidth needs and other constraints specified for the path, and the state of the network
- Path establishment: Establishing the cross-connects in each OXC in the computed route to realize the end-to-end path considering restoration, there could be *local* and *end-to-end* mechanisms for restoration of lightpaths within a subnetwork. Local mechanisms are used to select an alternate link between two adjacent OXCs when a failure affects the primary link over which the (protected) lightpath is being routed. Local restoration does not affect the end-to-end route of the light-path.

When local restoration is not possible (e.g., no alternate link is available between the adjacent OXCs in question), end-to-end restoration may be performed. With this, the affected lightpath may be rerouted over an alternate path that completely avoids the OXCs or the link segment where the failure occurred. For end-to-end restoration, alternate paths are typically precomputed. Such backup paths may have to be physically diverse from the corresponding primary paths. Physical diversity means that the primary and its backup paths should not be routed along facilities, which may be affected by the same failure. For end-to-end restoration, the primary and backup paths may be computed such that they do not contain links with the same shared link. Finally, end-to-end restoration may be based on two types of protection schemes: 1 + 1 or shared. Less than 1 + 1 protection, a backup path is established for the protected primary path along a physically diverse route. Both paths are active, and a failure along the primary path results in immediate switchover to the backup path. Under shared protection, backup paths corresponding to different physically diverse primary paths may share the same network resources. When a failure affects a primary path, it is assumed that the same failure will not affect the other primary paths whose backups share resources. Thus, the backup path for a primary path may be precomputed, but is activated only after failure of the primary path has been determined.

6.7.4 Optical Packet Switching

Research into optical packet switching (OPS) has been conducted over a number of years [41] [42]. Pure OPS, in which packet header recognition and control are achieved in an all-optical manner, is still years away. The objective of the OPS is to shift the bulk of the switching burden into the optical domain, permitting compatible scaling of the switching capability with WDM transmission capacity. Transmission and switching are executed in the optical domain, while routing and forwarding are carried out electronically, where the relatively complex packet header processing occurs independent of the optical payload. This decoupling effectively permits the optical packet layer to support a range of networking protocols while harnessing the power of WDM transmission. However, this is also changing, with the recent demonstration of rudimentary header processing functions directly in the optical domain [3]. These relieve some of the burden placed on electronic processing, thereby reducing control signal setup time and managing latency more effectively. With an extensive optical packet layer, the interface to IP and other protocols is crucial.

Encapsulation, the addition of delivery information to the data by the optical packet layer, will occur at interworking units (IWUs) at each interface to the electronic client layer. Encapsulation permits a range of protocols such as IP and asynchronous transfer mode (ATM) to be mapped into the optical payloads, which may be of either fixed or variable duration. IP hides the complexity of the physical layer (including optical packet switching), providing a unified interface to higher layers, regardless of the underlying network type. In addition to encapsulation, the IWUs create headers for proper routing within the optical packet layer, and multiplex traffic from different input links for onward transmission in optical packets for the same destination, ensuring an entirely optical end-to-end connection path. Optical packets provide a further multiplexing tier, allowing the aggregation of traffic flows prior to transmission over the optical layer, and also potentially obviating the need for SDH as an adaptation layer for IP traffic on WDM links. Optical packet networking therefore offers a potential solution to providing both connectionless and connection oriented networking capacities, flexible in terms of bandwidth management and future-proof with regard to bandwidth growth. No standards exist yet for mapping protocols such as IP and ATM into the optical packet layer. Thus, there are two principal approaches to optical packet switching, both with applications to the Internet:

- Employing fixed-length optical packets, with many corresponding to one IP datagram, requiring IWUs to fragment and reassemble the packets either at the edges of the layer or on the inputs and outputs of the switch
- Employing a variable-length optical packet for each IP datagram

6.7.5 MPLS based IP and WDM

The generality of MPLS architecture makes it applicable as a control/provisioning basis for various underlying data networking technologies [37]. MPLS decouples switching and forwarding capabilities, with packet forwarding decisions for resolving the end destination being performed only at the edges of the MPLS domain. The core utilizes high-speed packet/cell switching capabilities, such as ATM switching fabrics, to achieve faster data throughputs. Now recent optical advances have enabled a network-level role for WDM technology, with the emergence of dynamic wavelength switching and filtering capabilities. Moreover, complementary advances in MPLS-based frameworks for provisioning such wavelength capabilities have also emerged, such as multiprotocol lambda switching (MPλS) [43]. Recent efforts in the IETF are pushing this ubiquity further to include a full range of switching paradigms, even SONET/SDH circuits; namely, the generalized MPLS framework (GMPLS) [32]. Although MPλS has the potential to resolve the electronic routing bottleneck, it still poses several challenges. Perhaps the foremost concern is the capacity granularity issue, since the unit of bandwidth between edge node pairs of the MPLS domain is a full wavelength channel. Further more, due to its generality, GMPLS defines signalling/routing protocol extensions based on a generic label entity.

The earliest motivation of MPLS was to simplify wide-area IP backbone network architectures by overlaying IP over new emerging high-speed switching technology. Many standardization efforts have been devoted to developing packet label switching under the broader MPLS framework, with ATM as a sample underlying technology. MPLS concepts have been further extended to provision light-path circuit entities, to MPλS. A key to realizing MPλS is establishing a logical topology, as seen by upper-layer protocols i.e., IP in the current case. The logical topology consists of wavelength paths, which are configured over the WDM physical network, in order to carry IP packets utilizing the wavelength path. Here, the physical network represents an actual network consisting of the optical nodes and optical fiber links interconnecting nodes. Each optical node contains optical switch devices that can route an input wavelength to an output wavelength, such as optical cross-connect (OXC) or optical add-drop multiplexer (OADM) nodes. In many cases, these devices can preclude electronic processing, and hence a direct optical connection can be established between two endpoint nodes; this is referred to as a *lightpath* channel. By utilizing a logical topology consisting of lightpaths, even though the physical structure of the WDM networks is fixed, the logical topology now becomes the underlying network to the IP packet layer. In such a network, if the lightpaths are placed between every edge node pairs — ingress/egress packet label switch router (LSR) nodes according to MPLS terminology — no electronic processing is necessary within the network. In other words, the electronic router bottleneck can be avoided. An example of a logical topology is given in Figure 6.15, which illustrates a physical WDM network in which every link has two wavelength channels, λ1 and λ2. The logical topology shown in Figure 6.19 is then derived, and the logical view from IP is shown in Figure 6.20.

The core LSR nodes in regular MPLS can generally perform various operations on *packet* labels, including label swapping, label merging, and label stacking [43]. Clearly, it is difficult to realize those functions in the optical domain, since optical circuits are transparent to optical switching nodes. Perhaps an exception can arise if wavelength channels themselves are viewed as labels. Therefore, label swapping can be performed by changing an incoming wavelength to a different wavelength on the outgoing link at an optical node (OXC, OADM), as proposed in MPλS [23]. However, since wavelength conversion is still difficult/costly using current technology (i.e., required opto-electronic or transparent techniques), the functionalities of such MPλS nodes are relatively limited. In essence, a lightpath is set up in a circuit-switched fashion between ingress/egress (MPLS) *packet* LSR nodes (edge routers of the MPLS network). Now for IP routing, it is very natural that any-to-any connectivity is required among all the edge LSR nodes. However, this may require too many wavelengths, as shown in Figure 6.21.

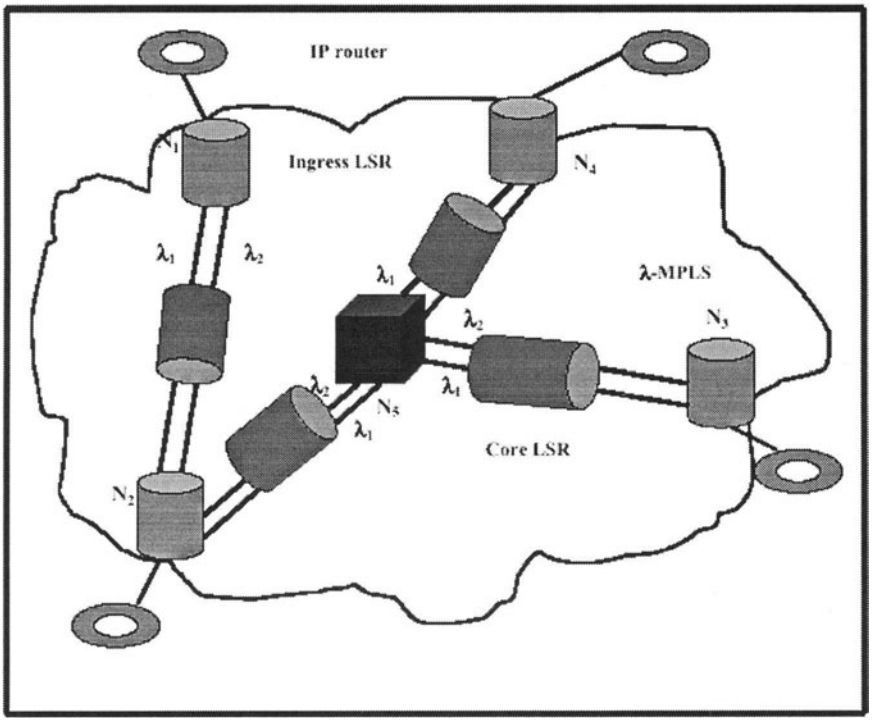


Figure 6.18 WDM physical topology

The packet forwarding capability at the IP layer is therefore necessary at the core LSR. The generic GMPLS framework facilitates this option of core LSR nodes having the capability of packet forwarding and lightpath switching. In particular, this can reduce the required number of wavelengths on the fiber, but requires additional packet processing delays in the electronic domain at the intermediate core LSRs. Thus, there is a clear trade-off relationship between the number of wavelengths multiplexed on the fiber and the required packet processing capability. Overall, once the logical topology is obtained, the following elements are necessary for MPλS operation:

- Ingress/egress electronic LSR nodes to map/unmap IP addresses to/from wavelength "labels."

•Label switched path (LSP) entities representing the lightpaths themselves.

•Core LSR nodes, comprising both optical lightpath switching and electronic packet forwarding capabilities. Specifically, an OXC switch will directly connect input and output wavelengths, whereas a packet forwarding capability at the IP layer will handle packets with different wavelength labels to share the same lightpath

•Label Distribution Protocol (LDP) to distribute labels and set up lightpath channels

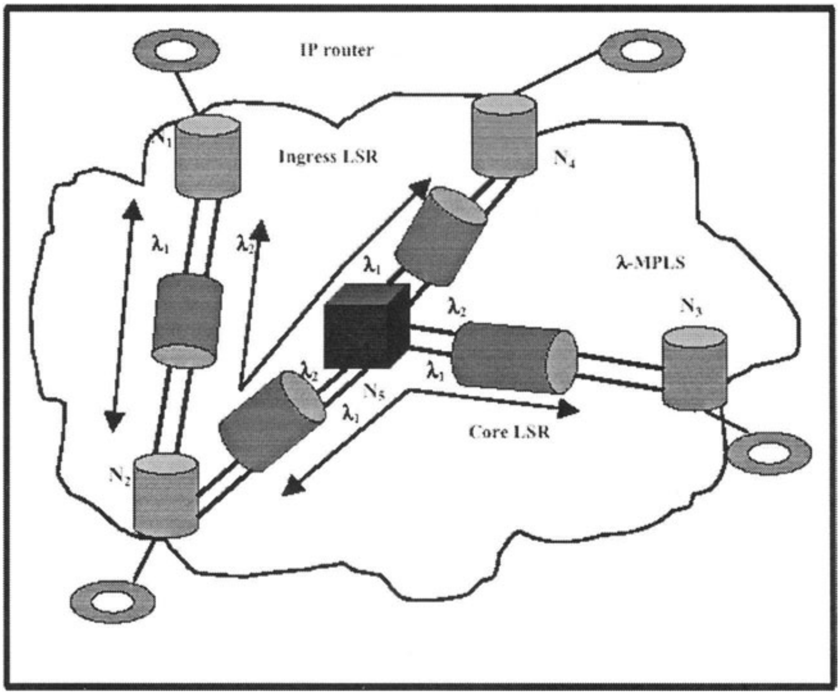


Figure 6.19 Logical topology consisting of three lightpaths

There are several challenges and concerns when operating MPλS networks. The first and perhaps most difficult problem is the capacity granularity issue. Now wavelength label merging and splitting in the optical domain are fundamentally difficult in a *circuit-switched* (MPλS) optical network, although some approaches are being investigated so far [32]. However, this is still a circuit-based solution, and hence may also suffer from the same capacity granularity problem, inflexibility, and decreased utilization of the large capacity of the wavelength-like entities.

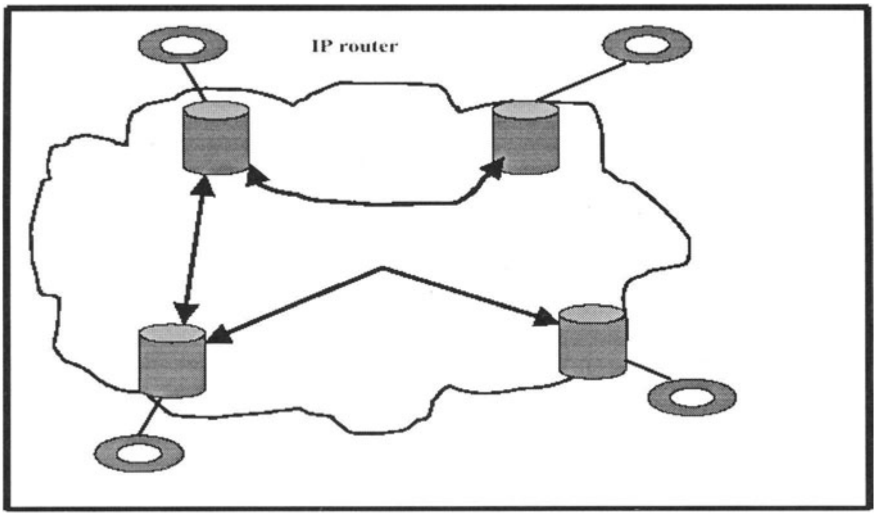


Figure 6.20 Logical views provided to IP

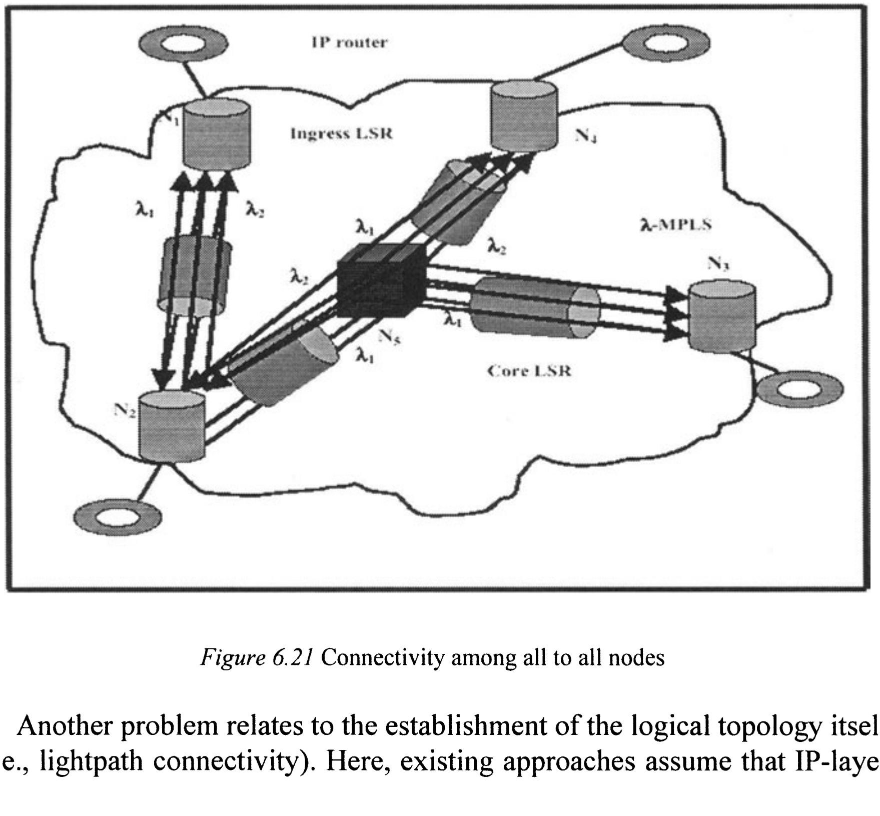


Figure 6.21 Connectivity among all to all nodes

Another problem relates to the establishment of the logical topology itself (i.e., lightpath connectivity). Here, existing approaches assume that IP-layer traffic load matrices are known a priori and compute the entire logical topology via the design algorithm. Now typically, it is unrealistic to expect that all IP-level traffic profiles can be characterized beforehand, since IP traffic and demand growth are highly variable. Although traffic loads may be estimated by direct traffic measurement, this implies that the traffic load can only be determined after the network is established and operated i.e., nonconducive to the a priori requirement.

6.8 INTERNET TELEPHONY

6.8.1 VoIP Mobility in Wireless Networks

Internet telephony, also known as voice over IP (VoIP), delivers real-time, two-way, synchronous voice traffic over the Internet or corporate intranets [44]. The dominant standard of Internet telephony is International Telecommunication Union- Telecommunication Standardization Sector (ITU-T) Recommendation H.323 [45]. H.323 specifies technical requirements for multimedia communications over packet-switched networks, including system components, control messages and functions for component communications, and services. Call setup and other call control signaling messages are carried out-of-band, sent through different paths from those for the payload traffic. VoIP mobility refers to mobility in the scope of IP telephony, where mobility may include terminal mobility, user mobility, and service mobility. Terminal mobility denotes the ability of a terminal to change physical location while the connection is still maintained. User mobility is defined as the ability to communicate regardless of the terminal type in use. Service mobility is the ability of a user to obtain a particular service independent of user and terminal mobility.

The existing activities in the international standards bodies toward VoIP mobility include European Telecommunications Standards Institute (ETSI) Telephone and Internet Harmonization over Networks (TIPHON) Working Group (WG) 7 and ITU-T Study Group (SG) 16, H.323 Mobile Annex. TiPHON mobility addresses user and service mobility for VoIP services, and supports the concept of *global multimedia mobility*, which assumes that future terminals may connect to several types of access networks, and the choice of access should be made dynamically according to individual needs [46]. H.323 allows interoperability between IP networks and the switched circuit network (SCN) through H.323 gateways, and hence may support a call across different cellular network types, say GSM to H.323 to Advanced

Mobile Phone System (AMPS). The current version of H.323, however, does not address interworking for cellular networks that is the part of the wireless SCN and IP networks. While H.324 gateways do support low-bit-rate transmissions- for example, public switched telephone network (PSTN), cellular phone- to H.323, the signals have to be transmitted through the PSTN to the H.323 system, making transmission inefficient.

6.8.2 H.323: An Overview

Inter-national Telecommunication Union- Telecommunication (ITU-T) Standardization Sector H.323 [47] covers the technical requirements for multimedia communications over packet-based networks that may not provide a guaranteed quality of service. Figure 6.22 illustrates an H.323 system. In this Figure 6.22 the terminal, gateway, gatekeeper, and multipoint control unit are called *endpoint*s.

The *terminal* is customer premises equipment that provides audio, video, and data communications capability in point-to-point or multipoint conferences in the H.323 network. The *gateway* performs call control functions (setup and release) and provides communication protocol translation mechanism between an H.323 endpoint and an endpoint of an external network such as PSTN, ISDN, or LAN. It also translates the transmitted media from one for-mat to another between the IP and circuit-switched networks. Two H.323 endpoints in the same network can communicate without involving the gateway. The *gatekeeper* is optional in an H.323 network, which may be physically collocated with a terminal, gateway, or multipoint control unit. A gatekeeper provides call control services to the H.323 endpoints. The functions of the gatekeeper include address translation, admission control, bandwidth control, and zone management. The gatekeeper may also perform optional functions such as call control signalling, call authorization, and call management. The *multipoint control unit* (MCU) utilizes multipoint controllers (and optionally multipoint processors) to support multipoint conferences. The *multipoint controller* (MC) provides control functions to support conferences between three or more endpoints in a multipoint conference. Every MCU contains an MC. Terminals, gateways, and gatekeepers may or may not contain MCs. The *multipoint processor* (MP) receives audio, video, and/or data streams from the endpoints involved in a multipoint conference. An MP is optionally included in a gateway, gatekeeper, or MCU.

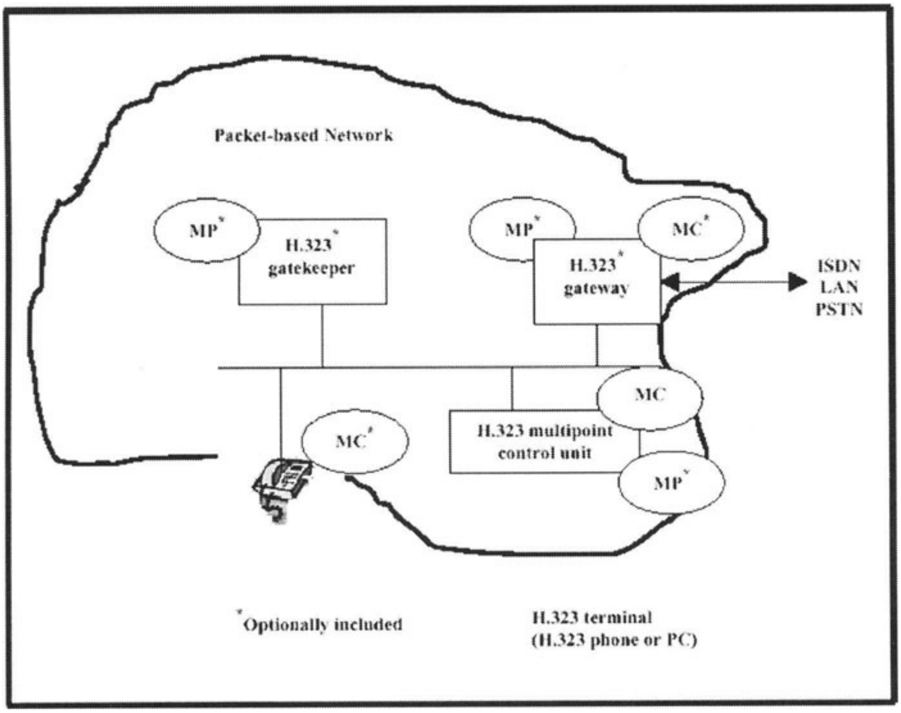


Figure 6.22 H.323 Architecture

6.8.3 Example Integration Scenario

A TIPHON scenario that integrates mobile and IP networks to support terminal mobility is shown in Figure 6.22, where the mediation gatekeeper serves as a VLR to support roaming management. The BSC/BTS in the IP network provides wireless access to the IP network. Another TIPHON scenario describes mobile and IP integration to support user mobility. We will elaborate on this scenario later.

Based on a concept similar to TIPHON, *GSM on the Net* [48] utilizes a corporate intranet, for example, to integrate an enterprise communications network with the public GSM network. This system supports user mobility where, by using various types of terminals, a user can move around the service area without losing contact with the system.

The *GSM on the Net* architecture is illustrated in Figure 6.23, and consists of GSM and corporate networks. The service node enables user mobility, controls calls among different types of terminals, and translates addresses between the PSTN and *Corporate intranets*. The access node resembles the MSC, VLR, and BSC. GSM/BTS provides the GSM MS with wireless access to the IP network. The gateway provides interfaces between corporate intranet and other networks particularly the GSM network.

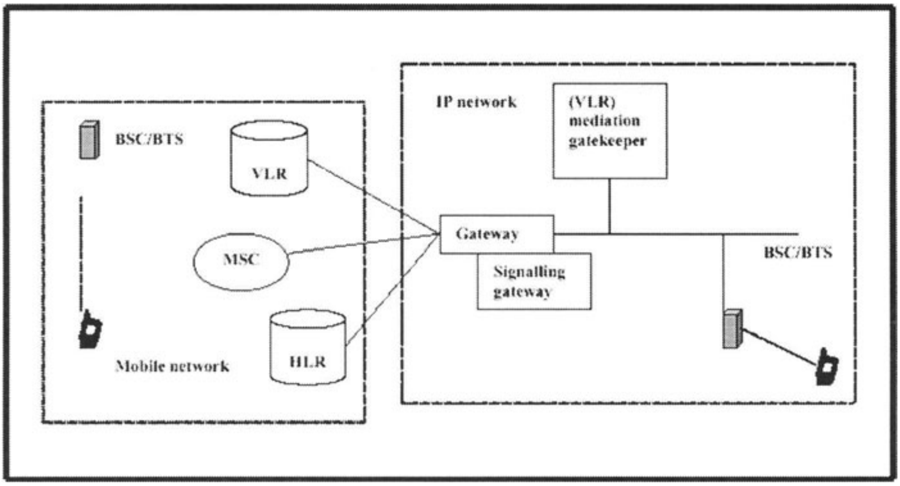


Figure 6.23 TIPHON IP and Mobile Networks integration

iGSM, a voice-over-IP value-added service for mobile network [48] is taken as an example case to explain VoIP service for wireless networks . The iGSM service provides user mobility to users, which allows them to use either GSM handsets or H.323 terminals (IP phones or PCs) to access telecommunications services.

This iGSM service realizes another TIPHON scenario that supports user mobility for GSM subscribers to access VoIP services. That is, a GSM user ordering the iGSM service enjoys the standard GSM services when he/she is in the GSM network. When the person moves to the IP network (without a GSM mobile station), he/she can utilize an H.323 terminal (IP phone or PC) to receive call delivery to his/her mobile station ISDN (MSISDN) number. The GSM roaming mechanism determines whether the subscriber is in the GSM or IP network. The iGSM system consists of GSM and H.323 (IP) networks. This is illustrated in Figure 6.25.

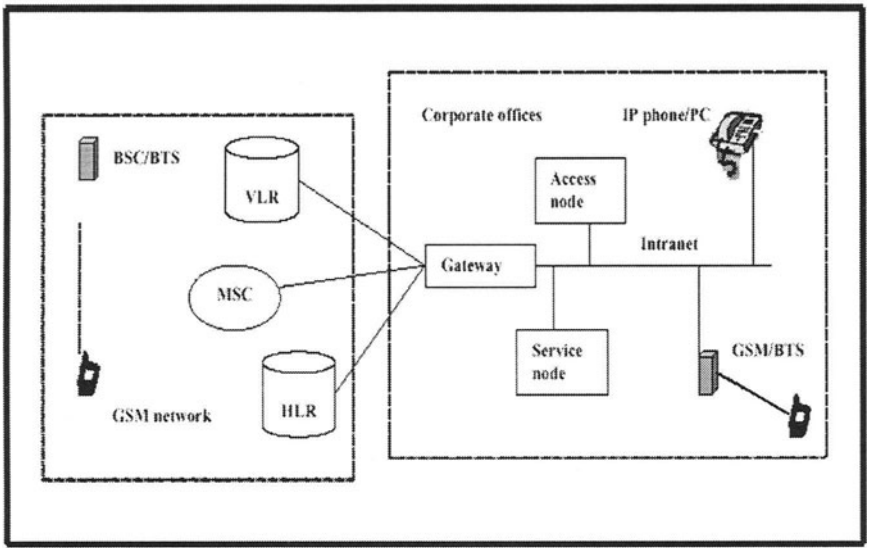


Figure 6.24 GSM Network and Corporate Intranet

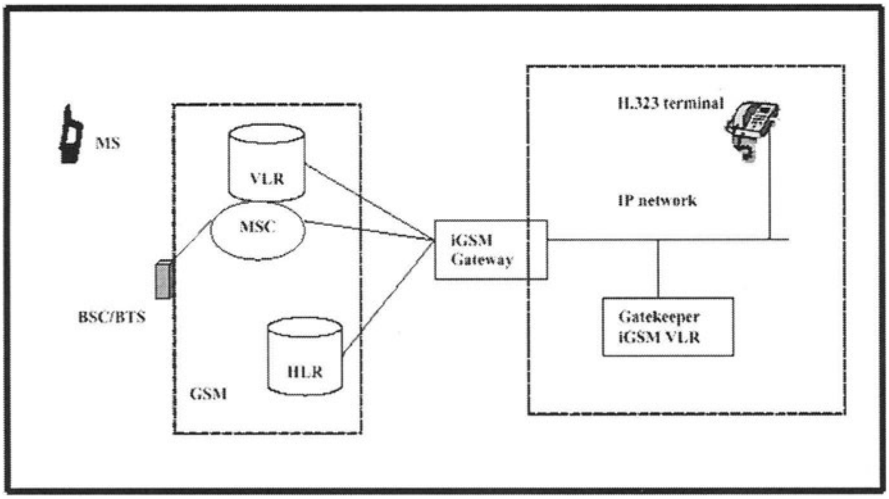


Figure 6.25 iGSM Architecture

6.9 ALL IP-BASED NETWORKS

PervNet infrastructures will consist of a set of heterogeneous networks using IP, enhanced IP or similar IP as a common protocol. In most cases, both wired and wireless networks will be used for a single communication session. IP mobility support will be an indispensable feature [50] of future mobile communications services in PervComp environment. Although both mobile communications and the Internet have been extremely successful during the last decade, the seamless integration of these two is still a great challenge in both areas. The current researches in this domain are based on the investigation how seamless IP layer mobility can be supported in 4G wireless infrastructures and subsequently enhancements to both Mobile IP and IP multicasting protocols are proposed. The IPv6 protocols, various enhancements to Mobile IP and similar IP are potential candidates of the "*pervasive IP*" as a seamless IP support in PervComp environment for a set of heterogeneous wired/wireless networks. The basic Mobile IP with its various enhancements for mobility management in telecommunication environments has the shortcomings [10].

The basic Mobile IP has large handoff delay if the MN and HA or CN are separated by many hops in a wide area network. Location updates need to travel over the entire path from the MN to the HA/CN before the change in mobile location is effectively communicated and ongoing connections are restored. Data in transit will be lost until the hand-off completes and a new route to the MN is established.

In different versions of Mobile IPv4 (with and without route optimisation) and in Mobile IPv6, location updates are always generated whenever the MN changes a subnet in the foreign network. Since subnet changes occur fairly rapidly, this approach results in frequent generation of location update messages. In situations with an extremely large population of MNs, the signalling load can become a significant portion of the traffic.

Although the recent work on tunnel management [51] talks about regional registration when the distance between the visited and home networks of the MN is large, it does not specify an architecture that is directly applicable in telecommunication environments. Moreover, in this scheme, not only is the assignment of a GFA (a stable globally valid care-of address) to a mobile performed by the FA, it is also suggested that the FA transparently append the GFA IP address information itself (as a registration extension) to the registration request message if the care-of address field is set to zero. We believe that practical implementation of such a mechanism would require the maintenance of valid security associations between all FAs and the HA, making the mobility management scheme significantly more complex. Finally, the idea of having the home network distribute the registration key associated with an MN to the corresponding GFA (to enable regional registrations in the visited domain) may weaken the strong security association paradigm between the HA and MN in conventional Mobile IP [52].

Mobile IP schemes that specify the use of a collocated care-of address implicitly assume the availability of a pool of public addresses. As MNs become ubiquitous, the availability of such addresses may become an issue. This is particularly relevant for cellular environments since providers may be unwilling to spend resources to obtain chunks of the public address space. Furthermore, the use of public addresses by arbitrary MNs within the provider's domain may be restricted or prohibited due to security concerns, firewall restrictions, and so on.

Since the current Mobile IP standard requires the mobile to change the care-of address (either FA or collocated) at every subnet transition, it is harder to reserve network resources on an end-to-end path between the CN and the mobile. For example, if Resource Reservation Protocol (RSVP) [26] is used to make reservations for quality of service (QoS) sensitive traffic, new reservations over the entire data path must be set up whenever the care-of address changes.

The preceding limitations are largely avoided in HAWAII or Cellular IP by ensuring that the MN maintains a single care-of address while changing subnets or cells within a domain. However, this is achieved at the expense of requiring the establishment of source-specific routes within the administrative domain. Such a proposal does not appear to be very scalable since the state information and route lookup complexity in the routers will increase rapidly with an increased mobile population. The propagation of source-specific routes within a single domain can significantly increase signaling complexity.

The Wireless IP network architecture (TR45.6) design uses existing standard protocols for mobility management and HLR/VLR for location update. Although this scheme offers some flexibility in routing by assigning a DHA in the visitor network, it requires protocol upgrades at all CNs, which may limit the market acceptance of this architecture.

The few upcoming research works tend to obtain *pervasive-IP* protocol to plug in shortcoming in the existing IP protocol and its various enhancements.

6.9.1 TeleMIP

The architecture of TeleMIP [10] is based on the observation that current IP mobility schemes have a subnet — and finer granularity of location resolution — and mostly no scooping for the transmission of location updates. Cellular IP [19], for example, proposes a base-station-level (layer 2) granularity similar to cellular networks. Its essence is derived from the *registration-are*a-based location management scheme currently employed in cellular networks. Such a scheme involves a combination of paging and location updates with a goal to minimize the overall cost by achieving an acceptable balance between these two kinds of traffic. Furthermore, in this architecture, it is assumed that BSs have layer 2 switching functionality similar to present-day cellular networks. Cellular IP [19], for example, proposes a base-station-level (layer 2) granularity similar to cellular networks.

The current subnet-based FA scheme in Mobile IP, on the other hand, leads to a change in care-of addresses at every subnet transition. In this architecture, it is proposed a generalization of the FA concept by introducing a new node, the *mobility agent* (MA), at network layer (layer 3) granularity, higher than that of a subnet, thus reducing the generation of global location updates. By limiting intradomain location updates to the MA, it is further proposed to reduce the latency associated with intradomain mobility without resorting to source-specific routes. Finally, our two-level mobility management scheme allows the use of private addressing (and, if necessary, non-IP mobility management) within the provider's own domain. See details in [10].

6.9.2 Enhancement in IP

In the PervComp environment, users will exchange information and control their environments from anywhere using various wireline/wireless networks and computing devices. Although IP protocols offer many technology independent solutions, such as DHCP, PPP and Mobile IP, current IP protocols must be enhanced to support PervComp [53]. In this proposed work [53] for *enhanced IP*, three such functions are identified: autoconfiguration, registration, and mobility management. The function autoconfiguration must be extended to configure routers and large unmanaged dynamic networks and describe one approach based on the Dynamic Configuration Distribution Protocol (DCDP). DCDP uses a top-down spanning tree-based distribution mechanism to rapidly configure an entire network with addressing information. This function also shows how network nodes to advertise and discover additional configuration and capability information can use the hierarchical distribution mechanism. Secondly, it is required for defining a uniform mechanism for users to register at a foreign network, independent of the choice of configuration and binding protocols. This is based on based on the Basic User Registration

Protocol (BURP) with its interface to AAA protocols. Thirdly, an aspect in this function has addressed the Dynamic Mobility Agent (DMA) architecture that provides a stable point of attachment within a network, and includes support for features such as QoS assurances, fast handoff and paging. Thirdly in the approach to mobility management, Dynamic Mobility Agent (DMA) based architecture provides a scalable solution for supporting seamless connectivity for a wide range of application classes. In particular, the various aspects are addressed: how the DMA architecture uses the Intra-Domain Mobility Management Protocol (IDMP) [54] to manage intra-domain mobility management and allows the use of multiple binding protocols (such as Mobile IP [52] or SIP [55]) for maintaining global reachability, and how this approach leverages existing IP-layer functionality to provide support for features, like fast handoffs, paging and QoS guarantees, that are important for providing mobility support to a diverse application set. Table I gives a snapshot of various network layer functions associated with supporting ubiquitous access and their current as well as the proposed solutions in the enhanced IP [53].

Table 6.2 Network layer functions in existing and enhanced IP [53]

Networking Function	Current approaches in existing IP	Proposed approaches in enhanced IP
Configuration	DHCP, PPP, manual Configuration	DCDP, DRCP
Registration	PPP, Mobile IP	BURP, AAA
Mobility Management	Mobile IP, SIP, layer-2 specific functions	Dynamic Mobility Architecture
QoS	Diffserv	BB based dynamic Diffserv (integrated with DMA)

6.9.3 All IP-based Wireless Networks

An IP device, with multiple radio interfaces or software radio, could roam between different wireless systems if they all support IP as a common network layer for wireline/wireless packet networks. Unlike today's radio systems that continue to depend heavily on proprietary technologies, IP provides a globally successful open infrastructure for services and applications. Such an all-IP wireless and wireline network could also make wireless networks more robust, scalable. All-IP wireless network configuration are IP-based wireless base stations (IBSs) connect radio systems to an IP radio access network [56]. IBSs use IP protocols for data transport and/or signalling (e.g., routing traffic based on IP-layer information, performing IP-layer mobility management, quality of service management, or service control functions). IBSs function in a distributed fashion as other IP network devices. They are interconnected via an IP network that may have any arbitrary network topology. Wireless cells, that are the geographical area covered by each IBS is a cell, may also be arranged in any arbitrary configuration. A key challenge in realizing such distributed all-IP wireless networks is how to support soft handoff. Handoff is a process that allows a mobile station's session in progress to continue without interruption when a MS moves from one cell to another. Soft handoff [57] allows MS to communicate with multiple BSs simultaneously. Several methods are available for supporting mobility in a wireless IP network. These include, for example, Mobile IP (IETF RFC 2002), Cellular IP [58], and HAWAII [59]. These methods provide ways for a MS to be handed off from one IP subnet to another. However, these methods focus on enabling hard handoff and do not address IP soft handoff issues explicitly.

Two major problems need to be solved in order to support soft handoff. First, multiple streams of the same IP traffic have to be distributed via multiple base stations to a mobile station. Second, pieces of data arriving at the mobile station at the same time from different base stations need to be copies of the same data in order for the mobile station's radio system to correctly combine these different pieces into a single copy. A similar problem also needs to be resolved in the reverse direction from mobile stations to base stations. Solving these problems in a distributed all-IP wireless network remains a challenge, although solutions exist for today's circuit-switched wireless systems. To tackle these problems [56]: first, a new design of IP-based distributed base stations enables mobile stations in multiple cells to be on the same IP subnet and multiple streams of the same data to be distributed via multiple base stations to a mobile without broadcasting/multicasting and with minimal signalling; second, IP-layer procedure performed by base stations ensure that the data coming simultaneously from multiple base stations to a mobile station are copies of the same data. These solutions do not impose any change to the protocols, software, and hardware used on a MS. A MS can use the existing radio technologies to perform signal combination for soft handoff and existing IP-layer protocols for IP-layer signalling and data transport.

6.9.4 IP-based IMT Network

The future IP-based techniques for the beyond IMT-2000 presents a vision for beyond IMT-2000 in terms of requirements for service and network capability [60]. The general architecture of the IP-based IMT Network Platform (IP^2) has considered few requirements for the establishments of this architecture [60].

Requirement 1: Multimedia Traffic

Multimedia traffic (e.g., data, image, video) will reach the same volume as voice traffic around year 2005 and then continue to increase much more rapidly. The increase will result in occupying 70–80 percent of all traffic. On the basis of this current rapid growth of the Internet or IT industry, most multimedia future traffic will be IP-based.

Requirement 2: Mobility Management

As the number of mobile users increases, the important issue in the mobile network is how to process mobility management efficiently. From now on, not only persons and vehicles but also other objects (e.g., delivery packets, vending machines, etc.) can be mobile users. IP^2 is required to flexibly manage mobility for such various mobile users.

Requirement 3: Radio Access Support

The 4G radio access is currently targeted to support at least 20 Mb/s. QoS levels (voice, unrestricted digital, etc.) will be supported in a packet-switched mode. IP^2 is required to support such diversified radio access features.

Requirement 4: Seamless Service

To date, roaming services have been implemented between mobile networks so that mobile users can communicate with their own telecommunication numbers in any visited networks. Moreover, the virtual home environment is being implemented so that mobile users can enjoy the same services in any visited networks as in their home networks. Thus, the network-seamless services have been offered in partnership only between mobile networks. IP^2 must implement network-seamless service capability between mobile networks and heterogeneous partners.

Requirement 5: Application Service Support

Many ASPs are utilizing mobile networks as a potential means to offer their services. Currently, most ASPs are connected to the wired Internet; in the near future, some ASPs may offer services from mobile terminals. IP^2 should form an environment to support their services under the extended ASPs.

The IP-based IMT Network consists of transport network and service middleware [60]. The transport network is IP-based to efficiently handle IP multimedia for *requirement* 1. Since all existing telecommunication networks are currently IP-oriented, IP-based transport is significant for network-seamless service for *requirement* 4. It is assumed that the IP transport network should be configured by routers and the service middleware configured by servers. Service middleware further consists of two layers, basic network management and service support. The basic network management layer includes radio resource management (RRM), mobility management (MM), call and session management (C/SM), security management, QoS management, and network operation and management (O&M) for basic mobile communication management. An IMT-2000 system is generally separated into the radio access network (RAN) and core network (CN). Therefore, mobility and routing are managed step-wise in the CN and RAN. In IP^2, routing and handover are managed from network gateway to MT in a unified IP-based way for *requirement* 2. Mobility is also managed in a unified manner over the entire IP^2. Conventional separation between RAN and CN is realized functionally by the boundary between territories where RRM and C/SM are applied. It is necessary to further study how clearly the basic network management layer can be separated from the IP-based transport network.

With unified mobility and routing management, IP^2 supports a wide variety of radio accesses such as 3G (W-CDMA), Bluetooth, ad hoc networks, wireless local loop, and 4G radio access, for *requirement* 3. The service support layer includes several service feature components. In addition, the IP^2 service support layer includes a mobile-specific component, location service support. These features are important for the terminal-seamless and contents-seamless services in *requirement* 4. These features should effectively work with the aid of the basic network management layer to add some additional value to the application services for *requirement* 5. Figure 6.26 shows a general architecture of IP^2 to meet the above five requirements.

6.9.5 All-IP-based UMTS Architecture

As the wireless industry is evolving its core networks toward IP technology, there is a need to develop standards, which are more global and collaborative. The global wireless industry has created two new global partnership projects, 3GPP [61] and 3GPP2 [62], to address the issue of the limited data capabilities of 2G systems and to start work on 3G and beyond wideband radio technologies that can provide higher data rates. Now that the radio technology standards to support higher data rates have been developed, the 3GPP and 3GPP2 are focusing on development of standards for all IP networks. Currently, 3GPP and 3GPP2 offer divergent proposals that need to be harmonized if convergence toward an IP-based mobile telecommunications networks is to become a reality.

There is a strategic group, IMT-2000 [63] within ITU which focuses its work on defining interfaces between 3G networks evolved from GSM on one hand and ANSI-41 on the other, in order to enable seamless roaming between 3GPP and 3GPP2 networks. To enable this seamless universal roaming characteristic, 3GPP started referring to 3G mobile systems as the Universal Mobile Telecommunication System (UMTS). In light of the recent evolutions in 3G standardization, the group of researchers investigates the synergy [64] between the two trends: on one hand, the trend in the design of the UMTS network architecture to move toward an all-IP approach, and on the other, the trend in the design of the UMTS service architecture to standardize open network interfaces. In this section it is to discuss an IP-based core network design on the UMTS service architecture toward a complete all-IP UMTS system architecture [65].

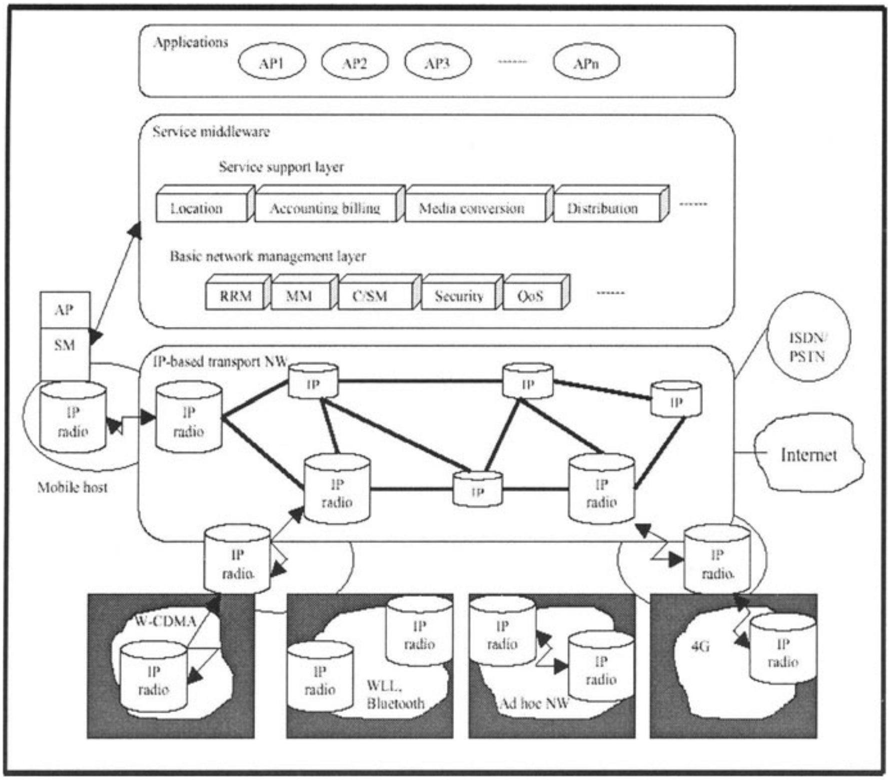


Figure 6.26 Architecture of IP-based IMT Network

The first release of UMTS will be based on the R99 specifications. The major innovation of R00 is the introduction of the IP multi-media domain. The following new features are introduced in Release 2000:

• Provisioning of IP-based multimedia services as an extension of the packet-switched services

•Enabling bearer-independent circuit-switched network architecture. Packet-based network transport replaces circuit-switched transport

• IP transport within the UTRAN

• Network architecture is independent of the transport layer, which can be based on either ATM or IP.

In the context of this article, an all-IP solution for UMTS refers to an all-IP core network (Figure 6.27).

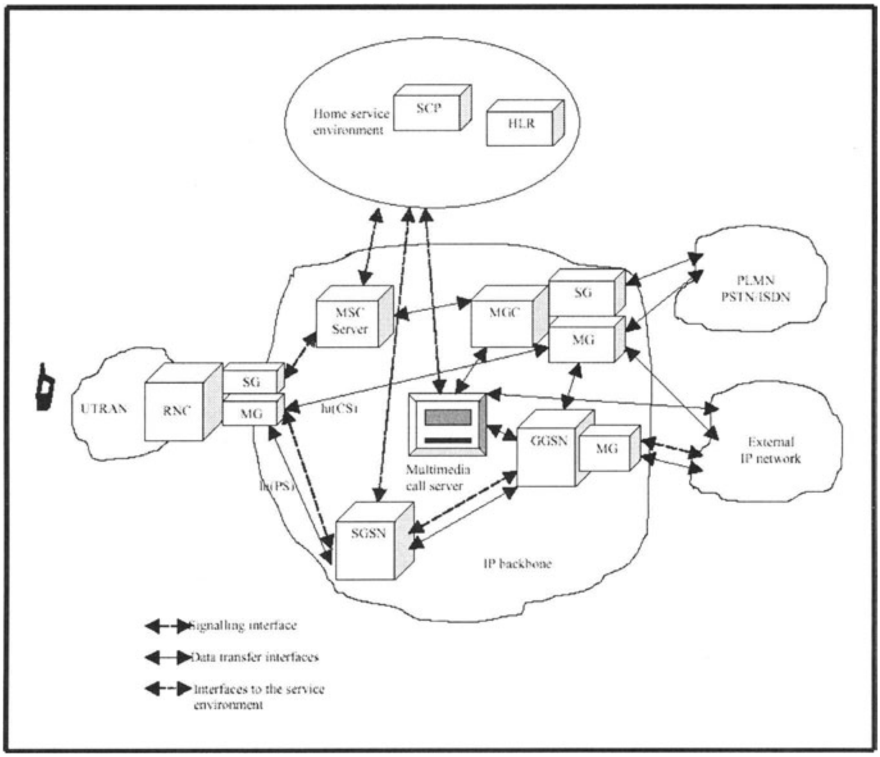


Figure 6.27 All-IP UMTS Architecture

The requirements for an all-IP core network are summarize as follows [65]:

• Support of roaming and handover to 2G networks (e.g., GSM, GPRS)

• Support of 3G circuit-switched terminals in a full IP UMTS core network, providing backward compatibility with R99 terminals.

• Support of new (e.g., IP and multimedia) as well as existing services, such as speech, SMS, and supplementary IN services.

The second requirement implies that there will be three types of 3G mobile terminals: circuit-switched, packet-switched (IP), and those that support both modes. Both circuit- and packet-switched modes are supported at the radio interface. The circuit-switched mode is used for traditional circuit-switched terminals and makes optimal use of the radio resources for voice services. The packet-switched mode is more flexible in terms of services supported and allows the introduction of multimedia applications, but is less efficient in terms of bandwidth consumption due to the IP header overhead over the radio. There are two major protocols for supporting VoIP: SIP, standardized by the IETF [66], and H.323, standardized by the ITU [45]. Figure 6.1 shows the proposed 3GPP all-IP UMTS core network architecture [65]. New elements in this architecture are:

- *MSC serve*r: The MSC server controls all calls coming from circuit-switched mobile terminals and mobile terminated calls from a PSTN/ISDN/GSM network to a circuit-switched terminal. The MSC server interacts with the media gateway control function (MGCF) for calls to/from the PSTN. R00 introduces the functional split of the MSC, where the call control and services part is maintained in the MSC server, and an IP router (MG) replaces the switch
- *Call state control function (CSCF)*: The CSCF is a SIP server that provides/controls multimedia services for packet-switched (IP) terminals, both mobile and fixed.
- *MG at the UTRAN sid*e: The MG transforms VoIP packets into UMTS radio frames. The MG is controlled by the MGCF by means of Media Gateway Control Protocol H.248.
- *MG at the PSTN sid*e: All calls coming from the PSTN are translated to VoIP calls for transport in the UMTS core network. This MG is controlled by the MGCF using the H.248 protocol.
- *Signaling gateway (SG)*: An SG relays all call-related signaling to/from the PSTN/ UTRAN on an IP bearer and sends the signaling data to the MGCF.
- *MGC*F: The first task of the MGCF is to control the MGs via H.248. Also, the MGCF performs translation at the call control signalling level between ISUP signalling, used in the PSTN, and SIP signalling, used in the UMTS multimedia domain.
- *Home subscriber server (HSS)*: The HSS is the extension of the HLR database with the subscribers' multimedia profile data.

The use of end-to-end IP sessions with higher bandwidths as in UMTS opens the path for mobile end users to a whole new set of multimedia over IP services such as videoconferencing, personal guidance systems, and network games. These services are believed to be some of the main drivers for UMTS beyond 3GPP specifically in PervNet environment. Using the same technology (i.e., IP services) in fixed and mobile networks facilitates interworking between both types of networks; also, the development and creation of new services is provided in a consistent way.

6.10 SUMMARY

The PervNet architecture reveals how to build this network out of a collection of heterogeneous networks, how to seamlessly roam around it and how to leverage computing in the infrastructure to enable users to have new abilities and services for even the simplest mobile devices. This network has broad coverage as a whole, but connection quality and services vary greatly from location to location. The connection would vary from wired or infrared in-room networks with great performance, to metropolitan cellular networks, to satellite networks with high latencies but tremendous coverage. Services vary greatly from home/office printer access, to local driving directions, to global services such as search engines and Web access [1]. In general, computation, storage, and complexity would be moved from the mobile devices into the infrastructure, thus enabling powerful new services, better overall cost performance, and small, lightweight, low-power, inexpensive mobile devices with tremendous functionality. The all-IP integrated wireless and wireline network could also make services and applications in PervNet more robust, scalable and cost effective.

In the vision of PervComp, users will exchange information and control their environments from everywhere using various wireline/wireless networks and pervasive devices. A wireless system, in general, is expected to provide *anytime anywhere* type of service while this feature is essential only for military, defense and few life-threatening areas like nuclear power, aviation, and medical emergencies. For most applications, *all time or everywhere* attribute may be adequate for the PervComp environment. Attempts should be made to move intelligence to the user side as much as possible and charges need to be based on service time and not purely on the connection time. Emphasis needs to be given on a scalable communication paradigm to connect wire/wireless networks over a *single* IP. There is also a need to characterize different kind of mobility, such as personal mobility, terminal mobility, service mobility, and corresponding effect on hand off in various layers need to be examined. To minimize handoff, the use of a macro-cellular infrastructure and multi-level overlapped schemes need to be investigated for users with different mobility characteristics. Multimedia needs a lot of bandwidth and a good mobility model is needed to characterize the traffic. The current protocols, such as DHCP, PPP and Mobile IP, Cellular IP, all existing IPs must be enhanced to support PervNet access. Therefore, a unified model is needed to represent voice and data over seamless *pervasive IP* (PIP, see Chapter 2).

With the success of the wired Internet, the next big challenge will be to extend the Internet and the applications to the mobile user in PervComp environment. There are many ongoing standardization activities to develop the respective wireless communications framework ranging from cellular wide Area (3G, 4G), Wireless LAN (IEEE 802.11, HomeRF) to Wireless PAN (IEEE 802.15, Bluetooth) to tune with users to run applications in the pervasive architecture (discussed in the next chapter). While the issues related to the communications within each wireless communications framework has been sufficiently addressed, there are still numerous open issues when it comes to their interoperability and integration with one another and with the Internet. The open issues [4], [49] are still untouched with respect to seamless IP across wireline/wireless communication environments. This is again confirmed by the recent considerable interest in pervasive extensions to the Internet from industry and academia.

REFERENCES

[1] Brewer Eric A., et.al. A network architecture for heterogeneous mobile computing. IEEE Personal Communications Oct 1998; 8-24

[2] Moral A.R., Bonenfont P., Krishnaswamy M. The optical internet: architecture and protocols for the global infrastructure of tomorrow. IEEE Communications Magazine Jul 2001; 152-59

[3] Yumiba H., Imai K., Yabusaki M. IP-based IMT network Platform. IEEE Personal Communications Oct 2001;

[4] Satayanarayanan M. Pervasive computing: vision and challenges. IEEE Personal Communications Aug 2001;

[5] Hinden Robert M. IP next generation overview. Communications of the ACM Jun 1996;

[6] Stallings Willam. IPv6: The new internet protocol.

[7] Perkins Charles E., Johnson David B. Mobility support in IPv6. Proceedings of Mobicom 1996

[8] Perkins Charles E. Mobile IP. IEEE Communications Magazine May 1997; 84-99

[9] Perkins Charles E. mobile IP joins forces with AAA. IEEE Personal Communications Aug 2000; 59-61

[10] Das S., et.al. TeleMIP: telecommunications-enhanced mobile IP architecture for fast intradomain mobility. IEEE Personal Communications Aug 2000; 50-58

[11] Montenegro G., Gupta V. Sun's SKIP firewall traversal for mobile IP. IETF RFC 2356; 1998

[12] Montenegro G. reverse tunnelling for mobile IP. IETF RFC 2344; 1998

[13] Caceres R., Padmanbhan V.N. Fast and scalable handoffs for wireless internetworks. Proceedings Mobicom. Aug 1996; ACM

[14] Perkins Charles E. Mobile IP local registration with hierarchical foreign agents. IETF Internet Draft. Feb 1996

[15] Johnson David B. Hierarchical foreign agents and regional registration. Minutes of the mobile IP working group meeting. IETF. Mar 1996

[16] Porta T La., Ramjee R., Li L. IP micro mobility support using HAWAII. Internet draft, draft-ietf-mobile ip-hawaii-00.txt; work-in-progress. June 1999

[17] MosquitoNet. Mobile IP resources. Technical report http://gunpowder.stanford.edu/mip/resource.html, 1998.

[18] Perkins Charles E., Calhoun P.R. Mobile IP network access identifier extension for IPv4. Internet draft; work-in-progress. July 1999

[19] Valvo A.G. Cellular IP: a new approach to internet host mobility. Computer Communication Review Jan 1999; 50-65

[20] Wan C.Y. Cellular IP. Internet draft; work-in-progress. Oct 1999

[21] Marthy L., Edwards C., Hutchison D. The internet: a global telecommunications solution. IEEE Network. Jul/Aug 2000; 46-57

[22] Black D., et.al. An architecture for differentiated services. IETF RFC 2475. Dec 1998

[23] Rosen E., Rekhter Y. BGP/MPLS VPNs. IETF RFC 2547. Mar 1999

[24] Braden R., Clark D., Shenkar S. Integrated services in the internet architecture: an overview. IETF RFC 1633. June 1994

[25] White P. Paul. RSVP and integrated services in the internet: a tutorial. IEEE Communications Magazine May 1997; 100-106

[26] Braden R., et.al. Resource reservation protocol (RSVP)- Version I functional specification. IETF RFC 2205, Sep 1997

[27] Moon B., Aghvani H. RSVP extension for real-time services in wireless mobile networks. IEEE Communications Magazine Dec 2001; 52-59

[28] Chen W.T., Huang L.C. RSVP mobility support: a signalling protocol for integrated services internet with mobile hosts. Proceedings INFOCOM 2000

[29] Chiruvolu G., Agarwal A., Vandenhoute M. Mobility and QoS support for IPv6 based real-time wireless internet traffic. Proceedings IEEE International Conference Communication, 1999

[30] Jain R., et. al. Mobile IP with location registers (MIP-LR). Internet draft, Jul 2001

[31] Shen Q., et.al. On providing flow transparent mobility support for IPv6-based real-time services. Proceedings MoMuc 2000; Tokyo, Japan

[32] Rosen E., Viswanathan A., Callon R. Multiprotocol label switching architecture. IETF RFC 3031. Jan 2001

[33] Lawrance J. Designing multiprotocol label switching networks. IEEE Communications Magazine Jul 2001; 134-142

[34] Awduche D. MPLS and traffic engineering in IP networks. IEEE Communications Magazine Dec 1999; 42-47

[35] Swallow G. MPLS advantages for traffic engineering. IEEE Communications Magazine Dec 1999; 54-57

[36] Muthukrishnan K., Malis A. Core MPLS/PVPN architecture. IETFRFC 2917. Sept 2000

[37] Banerjee A. et.al. Generalized multiprotocol label switching: an overview of routing and management enhancements. IEEE Communications Magazine Jan 2001; 144-50

[38] Armitage G. MPLS: the magic behind the myths. IEEE Communications Magazine Jan 2000; 124-31

[39] Ghani N., Dixit S., Wang T. On IP-over-WDM integration. IEEE Communications Magazine Mar 2000; 72-78

[40] Rajagopalan B., et.al. IP over optical networks: architectural aspects. IEEE Communications Magazine Sep 2000; 94-102

[41] Hunter D.K., Andonovic I. Approaches to optical internet packet switching. IEEE Communications Magazine Sep 2000; 116-22

[42] Mahony M J O., et.al. The application of optical packet switching in future communication networks. IEEE Communications Magazine Mar 2001; 128-35

[43] Oran D. OSI IS-IS intra-domain routing protocol. IETF RFC 1142

[44] Liao W., Lin J-C. VoIP mobility in IP/Cellular network internetworking. IEEE Communications Magazine Apr 2000; 70-75

[45] ITU-T Rec. H.323 v2. Packet-based multi-media communication systems. Mar 1997

[46] ETSI TIPHON. Analysis of existing roaming techniques applicable to TIPHON mobility services. TR101 338 v1.1.2. May 1999

[47] ITU-T Rec., H.450.1. Generic functional protocol for the support of supplementary services in H.323. Sep 1997

[48] Rao H.C.H, Lin Y-B., Cho S-Lin. iGSM: VoIP service for mobile networks. IEEE Communications Magazine Apr 2000; 62-69

[49] Weiser M. The Computer for 21st century. Scientific American Sep 1991

[50] Brin A., et.al. 4th generation wireless infrastructures: scenarios and research challenges. IEEE Personal Communications Dec 2001; 25-31

[51] Jonsson A., Gutafsson E. Perkins Charles E. Mobile IP regional tunnel management. Internet draft work-in-progress. Aug 1999

[52] Perkins Charles E. IP mobility support. IETF RFC 2002 Oct 1996

[53] Misra A., Das S. Mcauley A., Das S.K. Autoconfiguration, registration and mobility management for pervasive computing. IEEE Personal Communications Aug 2001;

[54] Misra A., Das S. Mcauley A., Das S.K. IDMP: an intradomain mobility management protocol using mobility agents. Internet draft work-in-progress. Jul 2000

[55] Wedlund E., Schulzrinne H. Mobility support using SIP. Proceedings of 2nd ACM int'l workshop on wireless mobile multimedia. Aug 1999. ACM/IEEE

[56] Zhang T., Agrawal P., Chen J-Cheng. IP-based base stations and soft handoff in all-IP wireless networks. IEEE Personal Communications Oct 2001; 24-30

[57] Garg V K. IS-95 CDMA and cdma 2000. Prentice Hall 2000

[58] Campbell A.J., Gomez J. Valko AG. An overview of cellular IP. Proceedings IEEE wireless communication network conference WCNC '99. 1999

[59] Ramjee R., et.al. HAWAII: a domain-based approach for supporting mobility in wide area wireless networks. Proceedings int'l conference network protocols. 1999

[60] Yumiba H. et.al. IP-based IMT network platform. IEEE Personal Communications Oct 2001; 18-25

[61] 3GPP home page. http://www.3GPP.org

[62] 3GPP2 home page. http://www.3GPP2.org

[63] ITU-R Draft Rec M. Detailed specifications of the radio interfaces of IMT-2000. Doc 8/126

[64] Bos lieve, Suresh Leroy. Toward an all IP-based UMTS system architecture. IEEE Network Jan 2001; 36-45

[65] 3GPP Technical Report 23.821 v 1.0.0. An architectural principles for R00. http://www.3GPP.org 2000

[66] Schulzrinne H. SIP: session initiation protocol. IETF RFC 2543 Mar 1999

Chapter 7

Wireless Standards

This chapter is related to Chapter 4 in the sense that wireless standards, which are either currently available or expected shortly, for the technologies, described in Chapter 4, are summarized here. This overview consolidates the proposition that the access shell of PervNet architecture (shown in Figure 2.2), is developing fast to realize the vision of PervComp.

7.1 INTRODUCTION

The concept of anytime, anywhere, anyone was realized by the development of mobile communications systems for voice communications. Data communication services through mobile networks have attracted many users to the WWW and have promoted the exchange of e-mail. These services are now expected to change people's lifestyles dramatically through further development of mobile communication technologies. Thus, the status of services of mobile communication systems is changing from handy phone to pervasive information infrastructure. Currently the Second-Generation (2G) wireless mobile system is under deployment all over the world. However, soon the Third Generation (3G) systems start replacing the 2G systems. Several versions and early 3G systems are almost available. The 3G system known as the IMT-2000, which has been introduced in 2001, will enhance the ability of data communications. The system offers channels of less than 2 Mb/s when subscribers move at vehicular speeds. Therefore, the mobile communications system beyond IMT-2000 (4G) would be designed to offer significantly higher bit rates than 2 Mb/s even in a vehicular environment and to adapt to data communications more efficiently to realize the concept of all time, everywhere, everyone, and everything from the viewpoint of pervasive communication.

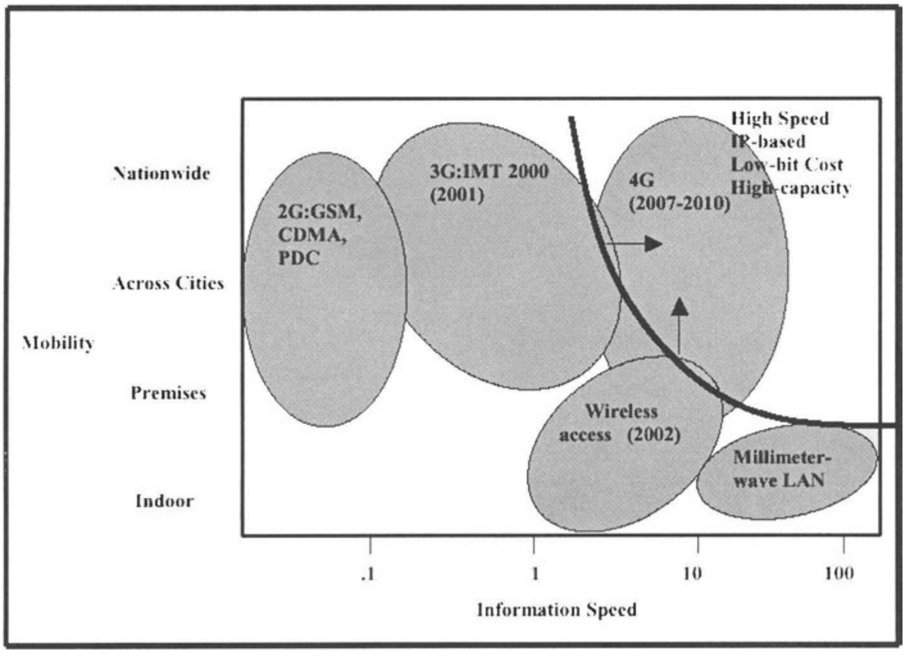


Figure 7.1 Capabilities of Mobile Systems

Taking a retrospective view of the history of mobile communications, it could be seen that a technological revolution in mobile communications or a major replacement in facilities has occurred every decade. Figure 7.1 shows [1] the capabilities of mobile systems and their application areas from the viewpoints of transmission bit rate and the mobility of terminals. As the figure shows, the milestones achieved in mobile communications aim at faster bit rates and wider service areas. The first-generation system, which was deployed in the 1980s, was based on analog FM transmission technologies; the second-generation (2G) system applied digital transmission IEEE technologies such as time-division (TDMA). Both generations are mainly used for voice communications, although the 2G system offers data communication services using digital channels at several tens of kilobits per second [1]. Nine radio transmission technology (RTT) proposals for 3G were submitted to the ITU during June 1998. Both time-division (TDMA) and code-division (CDMA) multiple access technologies have been proposed although the majority of the proposals were based upon wideband CDMA (WCDMA) technology. The WCDMA proposals are similar in many respects and may therefore be combined into at most two WCDMA proposals for the final ITU recommendation. The 3G system achieves a maximum bit rate of 2 Mb/s and will offer packet-switched multimedia services as well as circuit-switched voice services. Because the 4G system will most likely be introduced several years thereafter, a bit rate higher than that of the 3G system should be offered even in a high-speed mobility environment. From the aspect of other than the transmission bit rate, the 4G system will be expected to connect not only people but also machines and people in pervasive networking environment. In the 21st century our society will be more information-oriented and all information will be digitised and pervasive. Most electrical appliances will be equipped with communication functions. The ratio of data traffic to voice traffic will significantly increase. In addition, through enhanced mobile terminals such as PDAs (personal digital assistants), people will be able to access necessary information and control their appliances remotely whenever and from wherever they wish. In order to realize such a society, the 4G system would be designed to seamlessly connect people and their environment.

7.1.1 Wireless Generations

After the first-generation analog mobile systems, the second-generation (2G) mobile systems were introduced to the market around 1991. The shift from analog to digital and the rollout of new systems made the shift to the second generation very clear. The second-generation systems offered higher capacity and lower costs for network operators, while for the users, short messages and low-rate data services were added to speech services. Wide area roaming is another advantage, especially for GSM, which is available in almost all parts of the world. Presently, the 2G systems are GSM, TDMA, PDC, and cdmaOne. TDMA, cdmaOne, and GSM are all used in the U.S. GSM is used in most parts of the world except in Japan, where PDC is the second-generation system used (See Figure 7.2) [2].

A good example of an important evolution of the 2G systems, sometimes known as 2.5G, is the ability to use packet-switched radio connections over the air. For GSM systems, the packet switched solution is General Packet Radio Service (GPRS). The main investment for the operators lies in the new packet-switched core network, while the extensions in the radio access network mainly are software upgrades. For the users, GPRS offers the possibility to always be online and only pay for the data actually transferred. Data rates of up to 20 kb/s per used time slot will be offered, and with multiple time-slots per user in the downlink, attractive services can be offered.

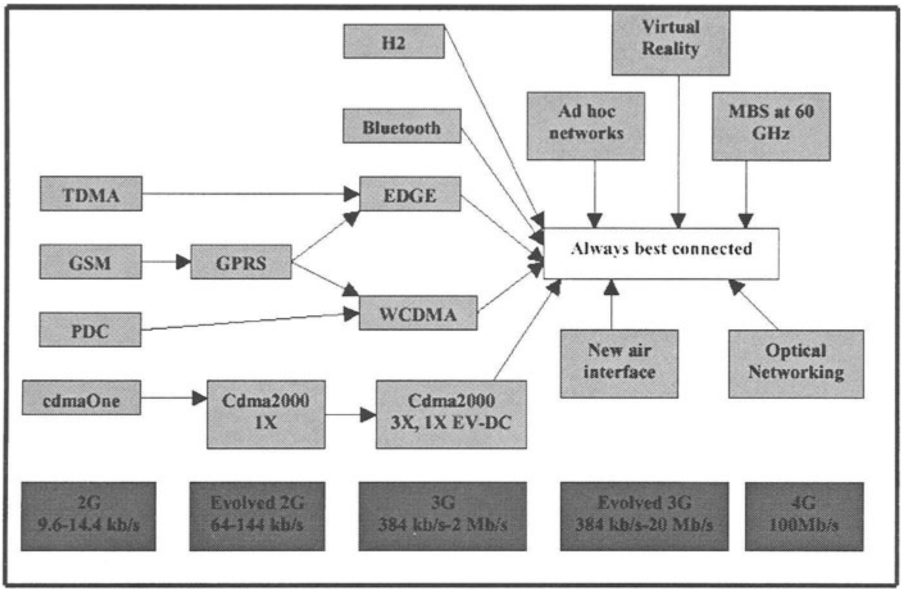


Figure7. 2 Generation of Mobile Systems

The shift to third-generation in the radio access networks is presently ongoing. The worldwide introduction of WCDMA has taken place in 2001 and 2002, starting in Japan and continuing in Europe. In the U.S., several 3G alternatives are available. GSM and TDMA operators can evolve toward EDGE, with WCDMA as a possible further step, while cdmaOne operators can evolve toward cdma2000 systems. WCDMA, as specified by the third-generation partnership project (3GPP), is a 3G system operating in 5 MHz of bandwidth. Variable spreading and multi-code operation is used to support a multitude of different radio access bearers. Different service classes are supported by an advanced quality-of-service (QoS) support. Data rates up to 384 kb/s for wide-area coverage and up to 2 Mb/s for local-area coverage are provided. For a system evolved as described in a later section, considerably higher peak rates are foreseen. EDGE is an evolution of GPRS with data rates of up to 60 kb/s per time-slot together with improved spectrum efficiency.

EDGE uses higher-order modulation together with link adaptation and incremental redundancy to optimise the radio bearer to the radio connection characteristics. Currently, additions in the form of a new set of radio access bearers to align EDGE toward WCDMA are being standardized within R5 of the 3GPP standards and are expected to be ready by the end of 2001. The same service classes as in WCDMA and the same interface to the core network will be used, the so-called lu interface. cdmaOne has evolved into cdma2000, and is available in two flavours, 1x and 3x. The former uses the same 1.25 MHz bandwidth as cdmaOne and supports up to approximately 600 kb/s, while the latter is a multi-carrier system using 3.75 MHz and supporting up to approximately 2 Mb/s. At the moment, the focus on 3x is very limited. As a complement to 1x, the standardization body 3GPP2 has recently specified 1xEV-DO (1x EVolution-Data Only). 1xEV-DO uses a separate 1.25 MHz carrier and supports best-effort data traffic only, using a new air interface compared to cdma2000. Voice traffic has to be carried on a separate cdma2000 carrier. The peak rate in the 1x EV-DO downlink is almost 2.5 Mb/s, excluding over-head. Phase two of the 1x evolution, known as 1x EV-DV (1x EVolution-Data and Voice) is currently being discussed within 3GPP2 and there are a number of proposals under consideration. The purpose is to specify an extension to cdma2000 1x in order to support high-rate data and voice on the same carrier.

At the same time as 3G standards are being introduced, other air interfaces have been developed and standardized. First of all, Bluetooth is already available, enabling devices to communicate over short distances. The strength of Bluetooth is low power consumption and a design enabling low-cost implementations. Bluetooth will be integrated into mobile phones, laptop computers, PDAs, and so forth. The first version of Bluetooth will offer up to 700 kb/s, but higher data rates, up to approximately 10 Mb/s, are currently being standardized for later releases. Wireless local area networks (WLANs) based on the different versions of the IEEE 802.11 standard have been around for some years in the 2.4 GHz ISM band. Data rates up to 11 Mb/s with reasonable indoor coverage have been offered. The next step in the WLAN evolution is the new systems developed for the 5 GHz band. Products based on two different standards, Hiperlan 2 (H2) and IEEE 802.11a, will be available starting in early 2002. The physical layers of the two are more or less identical, with a carrier spacing of 20 MHz, OFDM modulation, and data rates up to 54 Mb/s. The difference is the MAC protocol, where Hiperlan 2 has a more advanced protocol supporting QoS and mobility in a consistent way. Having defined WCDMA, EDGE, and cdma2000 as 3G technologies, and having recognized the presence and importance of Bluetooth and WLAN can be foreseen into two trends complementing each other. First, seamless roaming and hand-off possibilities between the above mentioned air interfaces. The second trend is the continuous development of the existing air interfaces. WCDMA, Hiperlan 2, and Bluetooth are all just in their beginning stages, with the first versions released in 2001–2002. Hence, the potential for improvements is large and many exiting new features will be standardized and available in products in the medium time frame, 2003-2005. Beyond 3G evolution are 4G mobile communication systems. At the moment different issues are being discussed in the research community and it is still unclear what will characterize 4G systems. One possible application driving the need of 4G systems could be augmented (virtual) reality applications, requiring high bit rates both in the radio interface and in the fixed network. Air-interface issues, ad hoc networking, and multihop networks are used as examples of 4G researches [2].

7.1.2 Mobile Communication Traffic

The amount of mobile communications traffic [1] will increase for a considerable time into the future based on the development of new pervasive applications. Mobile communications traffic in 2010 and 2015 estimated is based on the ITU-R report M.2023, "Spectrum requirements for IMT-2000," by ITU-R Task Group 8/1. The TG8/1 estimation classified services that will be available in 2010 into six categories according to the channel bit rate:

- Speech (16 kb/s in each direction)
- Simple message (14 kb/s in each direction)
- Switched data (64 kb/s in each direction)
- Medium multimedia (downlink/uplink: 384/64 kb/s)
- High multimedia (downlink/uplink: 2000/128 kb/s)
- Highly interactive multimedia (128 kb/s in each direction)

The amount of traffic is estimated by assuming the number of subscribers and frequency of use of each service category. "High multimedia" service, 2 Mb/s downlink and 128 kb/s uplink is the fastest service of the six categories. The amount of traffic of voice services that are representative services in the 1G and 2G systems is estimated to increase twofold in 2010 compared with that in 1999. Multimedia services will expand beyond those of voice in the 3G era and multimedia traffic will become twice that of voice services in 2010. To estimate the traffic in 2015, voice-service traffic will be saturated after 2010 multimedia traffic will grow at a 40 per-cent rate per year after 2010, and higher bit rate multimedia services will be introduced. The 40 percent increase rate is based on two factors:

- The capacity of memory and hard disks has increased at the rate of approximately 40 percent per year.
- The number of pixels in a CCD for input devices has also increased at the rate of about 40 percent per year.

Based on these assumptions, the amount of traffic in 2015 will be 23 fold that of the present, and multimedia traffic will account for 90 percent of the traffic. As indicated in this estimation, 4G systems should accommodate this dramatically increasing amount of multimedia traffic. Therefore, enhancing the system capacity as well as achieving a higher bit rate transmission is important requirements for the 4G system.

7.1.3 Wireless Transmission Characteristics

The 3G system [1] achieves a maximum bit rate of 2 Mb/s, but the bit rate may decrease in a vehicular speed environment. Wireless LANs and other broadband wireless access systems using 5-GHz frequency bands (e.g., MMAC [3], IEEE 802.11, and HiperLAN/2 [4]) will offer greater than 30-Mb/s-transmission capability in an indoor/pedestrian environment. For the 4G system, more than 20-Mb/s transmission will be realized in an outdoor/vehicular environment [5] [6].

Because the 4G system will provide greater than 20-Mb/s wireless channels and should accommodate the significantly increasing amount of traffic, sufficient frequency resources will be required. A lower frequency band, which is considered suitable for mobile communications, is now heavily used. Therefore it seems unlikely that a frequency band below 3 GHz will be used for the 4G system, although the frequency band for the 4G system has not yet been discussed in the ITU-R (WRC) [2].

Area Coverage —The 2G system now covers approximately 100 percent of populated areas, and customers can use mobile phones even in some buildings and underground shopping malls in urban areas. The 4G system is expected to have coverage similar to the 2G system. The 4G system will offer channels of more than 20 Mb/s, which is three orders of magnitude greater than that of the 2G system. The cell radius covered by a base station (BS) generally decreases if, assuming all other conditions are the same, radio signals are transmitted at higher bit rates because the received signal level must be higher than that at a lower transmission bit rate to compensate for the increased noise level. Moreover, the 4G system may be operated at a higher frequency band so that propagation loss of the wireless signal is higher than that of 2G and 3G systems. The increase in propagation loss caused by the operating frequency and channel speed can be converted into a decrease in cell radius [7]. If the transmission performance of the radio transmission scheme does not improve, the cell radius decreases to less than half of that of the 3G system when the operating frequency is 2 GHz and the channel bit rate is greater than 30 Mb/s, or when the operating frequency is 8 GHz and the channel bit rate is greater than 2 Mb/s. This means that to cover the same area as the 3G system, the 4G system will require four times the number of BSs. Furthermore, in order to accommodate the huge amount of traffic, the capacity of the 4G system should be increased to ten-fold that of the 3G system. Because frequency resources are limited, one solution to enhance the capacity is to decrease the cell radius of a BS.

Hierarchical Service Area — Although all objects will be connected to a network through wireless links, it may be difficult for small devices to be directly connected to the 4G system due to power consumption and antenna size. However, compact devices will be capable of exchanging wire less signals at short range. Therefore, compact devices will be able to access the 4G network through a miniature BS, which will act as a MT for the 4G system. By employing such a configuration, service areas will consist of multiple overlapping cells.

Seamless Connections — Imagining the network services in 2010, many types of wireless communication systems will be more popular as well as wired communications systems, and they will be used according to consumer needs [8]. The 3G system will play a major role in public mobile communication services, and wireless LANs will play a major role in private area communications. Short-range wireless systems will also be used to configure personal area networks (PANs). These PANs are very short-rang networks established around a person in which very closely dispersed personal devices for information or communication such as personal computers, PDAs, and mobile terminals exchange various types of information [9]. In addition to these wireless access systems, the 4G system will offer several tens of megabits per second channels for public mobile communications. When many types of networks can be used, customers may wish to access each system according to time, location, or other conditions. Concerns pertaining to the economic coverage of the 4G system of rural areas can be eased by the complementary use of other wireless systems. For these purposes, the following functions will be required:

- Interconnection between wireless access networks
- Capability of handover between wireless access networks
- Security mechanisms across wireless access networks

7.2 CELLULAR TELEPHONE SYSTEM

The evolution started in the early '90s with the replacement of the analog mobile network by the digital one, and is continuing today with the deployment of the third generation (3G). From circuit-driven networks we now enter the packet world through intermediate overlay networks, followed in years to come by all-IP networks. Global System for Mobile Communications (GSM) now accounts for about 66 percent of the world's total market. This market share is likely to increase as major time-division multiple access (TDMA) actors have started the move to GSM. The reason behind the TDMA migration to GSM is not only technical but also, and more important, financial thanks to GSM's huge economy of scale [7].

Another technological consolidation is occurring with 3G mobile technologies, where Universal Mobile Telecommunications System (UMTS) is the chosen evolution for all GSM networks, as well as for the Japanese

Personal Digital Cellular (PDC) network. As a result UMTS is the 3G choice of about 85 percent of mobile operators. Up to now, the growth of mobile phone users has been almost purely driven by voice services. Recently data has started to contribute at a considerable level to the revenues of mobile operators, reaching about 10 percent in the second quarter of 2001. Voice mobility is becoming a commodity for end users, and the market is demanding new applications in pervasive computing environment.

7.2.1 First-Generation Mobile Systems

Global System for Mobile Communications (GSM) now accounts for about 66 percent of the world's total market. During the early '80s, analog cellular telephone systems were deployed. At that time each country developed its own system, limiting usage within national boundaries and avoiding economies of scale. In most countries these systems were replaced by 2G systems during the '90s.

7.2.2 Second-Generation Mobile Systems

Currently, four 2G technology systems coexist: GSM, cdmaOne, TDMA, and PDC.

7.2.2.1 GSM

In 1989, GSM specifications [7] were made by the European Telecommunications Standards Institute (ETSI) and recently transferred to the 3G Partnership Project (3GPP). GSM commercial service started in July 1991, but handsets were really available only in the course of 1992. By 1993, there were 36 GSM networks in 22 countries, including non-European countries such as Australia and South Africa. In January 2002, there were more than 470 GSM operators in 172 countries with 646 million users. GSM allows up to eight users to share a single 200 kHz radio channel by allocating a unique time slot to each user. GSM is used in the 900 and 1800 MHz bands all over the world except North America (1900 MHz band). Soon, new frequencies will be used in the 450 and 850 MHz bands. Since its inception, GSM has been offering SMS, a connectionless packet service limited to messages containing less than 160 characters. Data transfers are also made possible using circuit-switched data (CSD), which offers throughput up to 14.4 kb/s. These limitations led to the standardization of the High Speed Circuit Switched Data (HSCSD) and General Packet Radio Service (GPRS). HSCSD enables higher rates (up to 57.6 kb/s), but like CSD is circuit-based. It is inherently inefficient for bursty traffic, continuously using several radio channels (up to four). The weaknesses of HSCSD mean that only around 30 operators have introduced it so far. Most operators use GPRS instead.

7.2.2.2 GPRS

GPRS, which keeps the GSM radio modulation, frequency bands, and frame structure, is designed around a number of guiding principles [8] [9]:

- Always on: Allows sending or receiving data at any time
- High bit rates: An actual bandwidth roughly equivalent to a wireline modem
- Improved usage of radio resources: Same radio channels shared between several users
- Separate allocation of uplink and downlink channels
- Simultaneous voice call and data transfer
- Billing based on volume

Figure 7.3 illustrates the GPRS system architecture. Compared to GSM, two new elements (shadowed objects) are introduced in order to create an end-to-end packet transfer mode. In addition, the HLR is enhanced with GPRS subscriber data and routing information. Two services are provided:

- Point-to-point (PTP)
- Point-to-multipoint (PTM)

Independent packet routing and transfer within the public land mobile network (PLMN) is supported by a new logical network node called the *GPRS support node* (GSN). The gateway GPRS support node (GGSN) acts as a logical interface to external packet data networks. The serving GPRS support node (SGSN) is responsible for the delivery of packets to the MSs within its service area. Within the GPRS network, protocol data units (PDUs) are encapsulated at the originating GSN and decapsulated at the destination GSN. In between the GSNs, the Internet Protocol (IP) is used as the backbone to transfer PDUs. This whole process is defined as *tunneling* in GPRS. The GGSN also maintains routing information used to tunnel the PDUs to the SGSN currently serving the MS. All GPRS user-related data needed by the SGSN to perform the routing and data transfer functionality is stored within the HLR.

Enhanced Data Rate for Global Evolution (EDGE) improves [7] GPRS by introducing a new radio modulation scheme that triples the bandwidth offered by GPRS. The EDGE upgrade has been started in 2002, mostly in the United States during the first phase. The GSM EDGE Radio Access Network (GERAN) group of 3GPP handles the further evolution of the GSM standard now. This group covers in particular the connection of GSM/ EDGE to 3G core networks and support of real-time services.

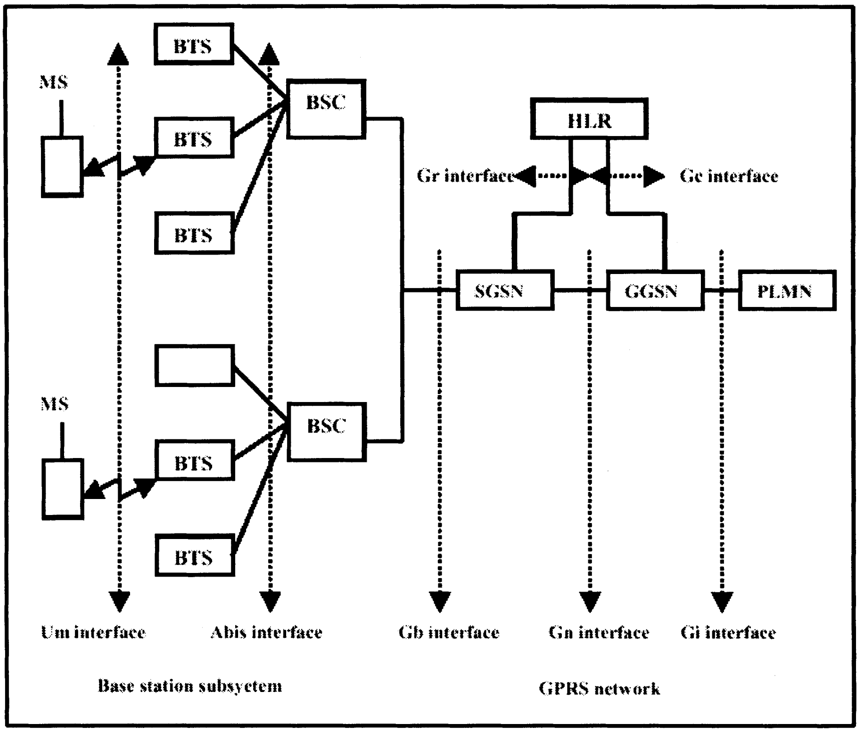


Figure 7.3 GPRS Architecture

7.2.2.3 cdmaOne

Spread spectrum technology [7] has been used in military applications for a very long time. In the mid-'80s, the U.S. military declassified this technology, and it was tested for cellular telephony applications.

The spread-spectrum-based code-division multiple access (CDMA) standard, was approved in July 1993 by the Telecommunications Industry Association (TIA). With CDMA, unique digital codes, rather than separate RF frequencies or channels, are used to differentiate subscribers. The codes are shared by both the mobile station (cellular phone) and the base station, and are called "pseudo-Random Code Sequences." CDMA commercial networks opened in 1995, but by mid-1998 had attracted only 9 million users. Things have improved since that time, with today around 100 million users, mostly in the Americas (55 million) and Asia (40 million). CDMA is now called cdmaOne to differentiate it from 3G CDMA systems.

With CDMA, many users (up to 64) share the same 1.25 MHz channel. Attaching a pseudo-random code to each user allows decoders to separate traffic at each end. All base stations transmit the same pseudo-random code with a time offset; therefore they must remain synchronized.

CDMA is used in the 850 MHz and the 1900 MHz bands. Like GSM, IS-95A, the first version of CDMA, offers throughput limited to 14.4 kb/s. All users share the same range of radio spectrum. In June 1997 IS-95B CDMA specifications were completed. By assigning up to seven supplementary codes in addition to the fundamental code, data rates up to 64 kb/s are possible. Some Asian operators have started to implement IS-95B CDMA offerings.

The cdmaOne packet data implementation, on the other hand, utilizes standard routers, which are the same ones used in the landline Internet. cdmaOne networks are based on IP standard and use IP addressing within the network without the need for an additional IP layer being added to the packet transport layer. This allows for a high degree of backward and forward hardware compatibility for network operators looking to implement new higher speed data services and evolve to 3G, which is an IP-based standard. Today's cdmaOne networks already incorporate an IP gateway referred to as the Inter-Working Function (IWF). This is essentially a standard IP router built into the network, routing IP packets without the need for them to be handled by an analog modem. The IWF receives information from the mobile phone in Point to Point Protocol (PPP) format and assigns a temporary IP address for that session. Current cdmaOne phones have the standard IP protocols built into the handset.

7.2.2.4 GPRS vs. cdmaOne Packet Data

The path to high-speed packet data differs greatly between GSM and cdmaOne networks. GSM network requires a new data backbone, base station upgrades and new handsets to offer packet data services. Packet data in cdmaOne networks is standard and was built into the IS-95 standard from its inception. All cdmaOne handsets and base stations are packet data capable today, and the networks utilize standard Internet protocol (IP) based equipment. GSM is circuit- based, requiring a new packet data backbone and new handsets, the commercial launch of which has been delayed until early 2001. The next major upgrade for GSM is GPRS, which is 2.5G, while the next major upgrade for cdmaOne is 1X, which is 3G. One of the most critical factors is the forward and backward compatibility of the handsets--the capability of an older handset to operate on an upgraded network and the capability of a newer handset to operate on an older network. The Second factor is the cost and ease of integration of the packet data network and the ability for third parties to implement services on these data backbones to offer high-speed Internet services.

Table 7.1 GSM Path

Packet data Equipment requirements	GSM CSD	GPRS	EDGE	IMT 2000 CDMA Direct Spread (CDMA DS)
Handset	No packet data capability - Single-Mode phones	New handsets GPRS-- enabled handsets will work on GPRS enabled networks and 9.6Kbps on GSM networks using CSD-Dual Mode phones	New handsets EDGE-handsets will work at up to 384Kbps on EDGE enabled networks on GPRS enabled networks and 9.6Kbps on GSM networks using CSD-Tri-Mode phones	Modulation changes required to GSM TDMA platform
Infrastructure	No packet data capability	New packet overlay/ backbone needed for circuit switched network	Further backbone modifications required	New infrastructure roll out with existing interconnect
Technology Platform	No packet data capability	GSM TDMA platform with additional packet overlay	Modulation changes required to GSM TDMA platform	New CDMA infrastructure

The GSM data evolution path will always require new network infrastructure and new phones. GSM also requires the implementation of IP based network elements to allow a packet overlay onto a circuit switched network. The links between the existing GSM network infrastructure entities and the IP backbone are comprised of proprietary hardware such as the Gateway GPRS Service Nodes (GGSNs) that link the Internet to the IP backbone. These are MODIFIED IP routers. The cdmaOne packet data implementation, on the other hand, utilizes standard routers, which are the same ones used in the landline Internet.

GPRS has a disadvantage in that the initial GPRS capable mobile terminals are expected to support only a maximum of four simultaneous channels. GPRS and voice both use the same traffic channels, meaning that

that both voice and data are competing for the same resource. EDGE has a maximum theoretical data rate of 384 kbps, but EDGE works in a similar way to GPRS in that this would require all 8 timeslots to be available to a single user who would also need to be given priority over voice. CDMA 1X will allow approximately 90% throughput of the implemented bandwidth to the application layer and offers user rate of 130 kbps.

Table7.2 CDMA Path

Packet data Equipment requirements	95A	95B	IMT-2000 CDMA Multi-carrier 1X (MC 1X)	IMT-2000 CDMA Multi-carrier 3X (MC 3X)
Handset	Standard 95A handsets will work on all future networks: 95B, 1X and 3Xat 14.4Kbps-Single-Mode phone	Standard in chipsets 1999 95B handsets will work on 95A networks at 14.4Kbps and 95B, 1X and 3X systems at speeds up to 114 Kbps-Single-Mode phone	1X standard in chipsets in 2001 1X handsets will work on 95A networks at 14.4Kbps, 95B Networks at speeds up to 114 Kbps and 1X and 3X networks at speeds up to 307Kbps-Single-Mode phone	New handsets 3X handsets will work on 95A networks at 14.4Kbps, 95B networks at speeds up to 114Kbps and 1X networks at speeds up to 307 Kbps and 3X networks at 2Mbps-Single-Mode phone
Infrastructure	Standard	New software in BSC (Base Station Controller)	1X requires new software in backbone and new channel cards at base station	Backbone modifications New channel cards at base stations
Technology Platform	CDMA	CDMA	CDMA	CDMA

7.2.25 TDMA

With analog cellular systems, such as Advanced Mobile Phone Service (AMPS), a single subscriber at a time is assigned to a 30 kHz channel. D-AMPS, the TDMA system designed to coexist with AMPS systems, divides this 30 kHz channel into three channels, allowing three users to share a single radio channel by allocating unique time slots to each user. Recent developments show that the TDMA community is moving toward GSM. These new GSM networks integrate GPRS and EDGE. Deployment of UMTS requires additional spectrum and be limited to 3G operators gaining new frequencies.

7.2.2.6 PDC

PDC is the Japanese TDMA-based standard operating in the 800 and 1500 MHz bands. PDC hosts the most convincing example of mobile Internet, iMode. The congestion of the PDC system urged NTT DoCoMo to replace it rapidly with a 3G system.

7.2.3 Third-Generation Mobile Systems

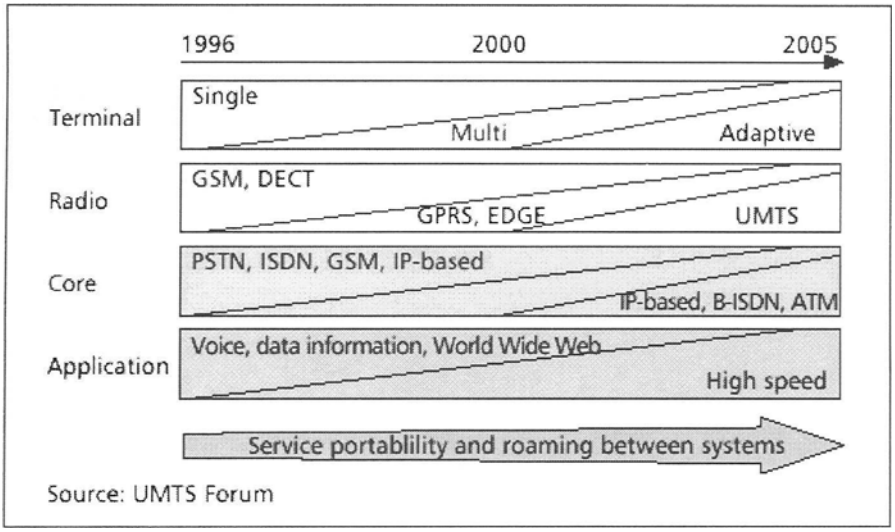
Third-generation mobile radio systems-International Mobile Telecommunications in 2000 (IMT-2000) in the International Telecommunication Union (ITU) and Universal Mobile Telecommunications Service (UMTS) in Europe-are currently being standardized and deployed worldwide. Their main goals are to support broadband data services up to 2 Mb/s with a wideband radio interface, and international roaming for circuit-switched and packet-oriented services (see Figure 7.4) [10]. These systems aim to integrate different second-generation cellular and cordless services. IMT-2000 supports time-division duplex (TDD) and FDD to enable asymmetric and symmetric data services in a spectrally efficient way. The transport in the radio access network is based on asynchronous transfer mode (ATM) and IP [11] [12]. IMT-2000, which is optimized for data services, will open new business opportunities such as seamless and bandwidth-on-demand services. At the end of 1999 the ITU - Radio communication Standardization Sector (ITU-R) approved the specifications of the IMT-2000 radio interfaces, which are part of the IMT-2000 family [13].

The terrestrial component of IMT-2000/UMTS comprises:

- Direct spread CDMA based on the Third Generation Partnership Project (3GPP) concept [13]- Wideband CDMA (WCDMA), also called frequency division duplex (FDD)
- TDD (time division duplex) CDMA based on the 3GPP concept and the Chinese concept from CWTS [12] [13]
- Multicarrier CDMA based on 3GPP2 [13]- cdma2000 that is the evolution of cdmaOne
- Single-carrier TDMA based on the evolution of ANSI-136 with EDGE and a high-speed mode [13]

- Multicarrier TDMA based on the DECT concept [13]

Third-generation mobile radio systems are deployed starting in 2001.



Source: UMTS Forum

Figure 7.4 Technological trends on the way to IMT-2000 / UMTS

7.2.3.1 UMTS

Technical specification work on FDD and TDD standardization is being done within the 3GPP [7]. The edition of specifications is phased in different releases:

3rd Generation Partnership Project (3GPP) [14] is developing 3G standards for GSM-based systems. The consortium includes ETSI, T1 (North America), Association of Radio Industries and Businesses (ARIB)/TTC (Japan), Telecommunications Technology Association (TTA) (Korea), and CWTS (China). The North American TDMA community is participating and contributing in 3GPP as American National Standards Institute (ANSI)-41-based TDMA systems evolve toward 3G architecture based on EDGE and General Packet Radio Service (GPRS).

- 3GPP release 3 specifications, formerly called release '99, define FDD and TDD modes, and are based on asynchronous transfer mode (ATM) in the radio access network. Release 3 was actually issued in March 2000 and became stable in June 2001.
- 3GPP release 4 specifications define a new version of TDD and FDD mode improvements. Release 4 was frozen in March 2001.

- 3GPP release 5 specifications includes IP-based transport within the radio access network. Release 5 is scheduled for March 2002. FDD mode is considered the main technology for UMTS. FDD mode is derived from CDMA and also uses pseudo-random codes. Separate 5 MHz carrier frequencies are used for the uplink and downlink, respectively, allowing an end-user data rate up to 384 kb/s (2 Mb/s per carrier). Later on, high-speed downlink packet access (HSDPA) will allow downlink data rate transmission to increase. FDD allows the operation of asynchronous base stations.

The TDD mode likely to be deployed is time-division-synchronous code-division multiple access (TD-SCDMA). TD-SCDMA operates on low-chip-rate carriers, with 1.6 MHz carrier spacing instead of 5 MHz for the other wide-band standards. It allows end-user data rates up to 2 Mb/s in optimal conditions. NTT DoCoMo commercialised a 3G service, called FOMA, in October 2001. Elsewhere, the installation of the first UMTS system (FDD mode only) will start in 2002, and marketing of services during 2003.

7.2.3.2 Cdma2000

3rd Generation Partnership Project 2 (3GPP2) [15] is developing 3G standards for CDMA systems. The consortium includes TIA, ARIB/TTC, TTA, and CWTS. Technical specification work forcdma2000 standardization is being done within 3GPP2 in the following steps [7]:

- cdma2000 1x, which is an evolution of cdmaOne, supports packet data service up to 144 kb/s.
- cdma2000 1xEV-DO introduces a new air interface and supports high-data-rate service on downlink. It is also known as high rate packet data (HRPD). The specifications were completed in 2001. It requires a separate 1.25 MHz carrier for data only. 1xEV-DO provides up to 2.4 Mb/s on the downlink (from base station to terminal), but only 153 kb/s on the uplink. Simultaneous voice over 1x and data over 1xEV-DO is difficult due to separate carriers.
- cdma2000 1xEV-DV, which will introduce new radio techniques and an all-IP architecture for radio access and core network. The completion of specifications is expected in 2003. It promises data rates up to 3 Mb/s. SK Telecom from Korea were the first operator to launch cdma2000 1x in October 2000. Since that time, only a few operators have announced cdma2000 1x service launches. Some operators recently announced setting up cdma2000 1xEV-DO trials.

7.3 EVOLUTION OF THE NETWORK ARCHITECTURE

The second-generation network architecture of GSM/GPRS has already been discussed in the earlier section.

7.4 UMTS Network Architecture

The UMTS release 3 network consists of two independent subsystems connected over a standard interface (see Figure 7.5) [7].

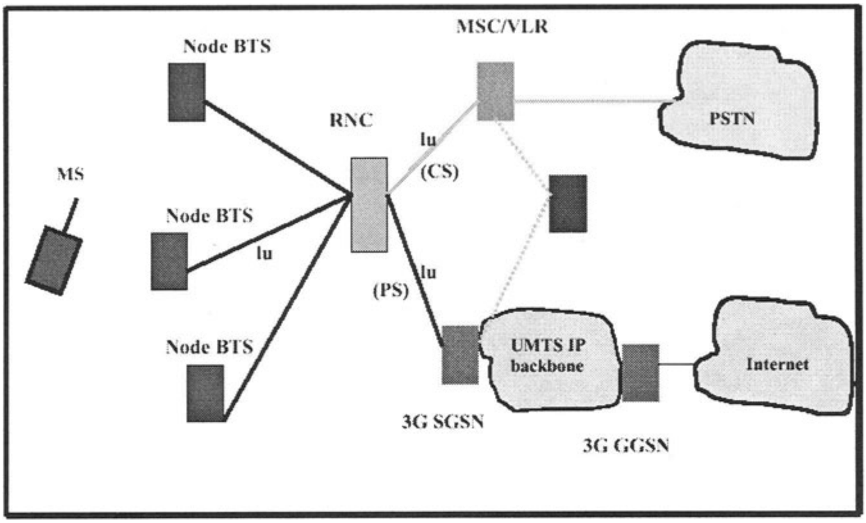


Figure 7.5 UMTS Network

- UMTS terrestrial radio access network (UTRAN) composed of node BTS a radio network controller (RNC). Node BTS is functionally similar to the GSM BTS, and RNC is similar to the GSM BSC.
- UMTS core network is equivalent to the GSM/GPRS NSS. The UMTS core network reuses as far as possible the GSM/GPRS NSS.
- Packet switch (PS) is an evolution of the GPRS SGSN/GGSN with a more optimised functional split between the UTRAN and core network
- Circuit switch (CS) is an evolution of the NSS with the transcoder function moved from the BSS to the core network. As described earlier, UMTS is based on a new radio technology having a big impact on the UTRAN.

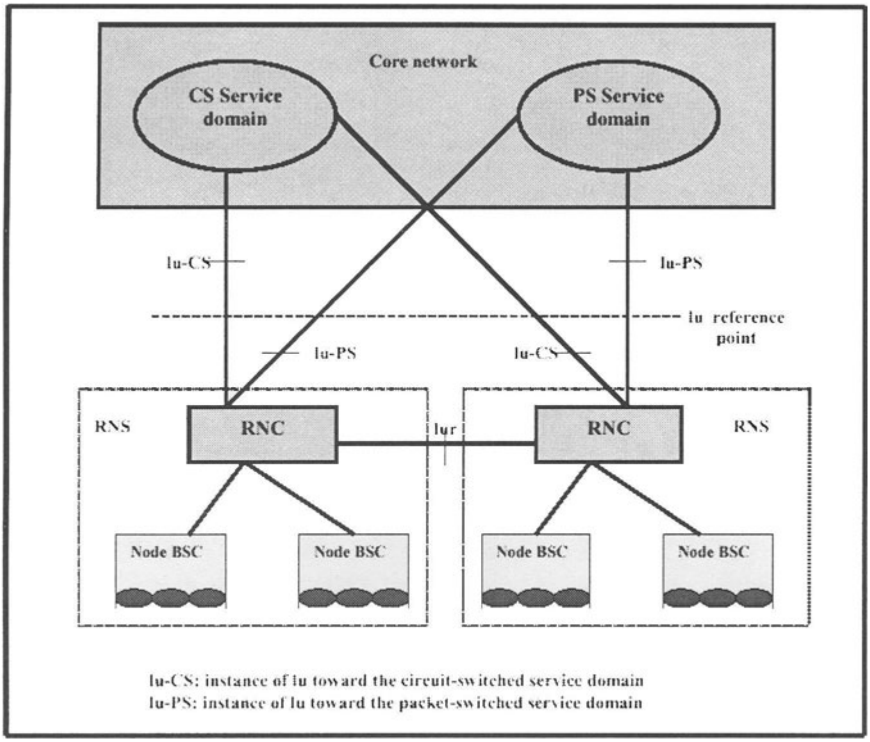


Figure 7.6 UTRAN Architecture

The UTRAN (Figure 7.6) [7] consists of several possibly interconnected radio network subsystems (RNSs). An RNS contains one RNC and at least one node BTS. The RNC is in charge of the overall control of logical resources provided by the node BTSs. RNCs can be interconnected in the UTRAN (i.e., an RNC can use resources controlled by another RNC) via the Iur interface. Node BTS provides logical resources, corresponding to the resources of one or more cells, to the RNC. It is responsible for radio transmission and reception in the cells maintained by this node BSC. A node BTS controls several cells. At a later stage, an evolution of EDGE called GERAN will allow upgrading 2G infrastructure to offer UMTS capabilities such as real-time packet services. The UMTS functional split between BSS and core network will be applied to GERAN with the current assumption of a transcoder located in the core network.

7.3.2 UMTS All-IP Architecture

At the end of 1999, work started in 3GPP toward an all-IP architecture [7]. This evolution was driven by two objectives:

- Independence of the transport and control layer to ease the implementation of new applications up to the mobile terminal
- Operation and maintenance optimisation for the access network

This evolution has an impact on different parts of the network. Basically, three main (and independent) evolutions are part of this evolution toward an all-IP architecture:

- Evolution moves toward a next-generation network (NGN) type of architecture in the CS domain, where the MSC function is split into a control plane part (MSC server) and a user plane part (media gateway). The introduction of packet transport (IP or ATM since the network architecture is independent of the underlying transport layer) on the NSS backbone also allows moving the transcoder toward the border of the public land mobile network (PLMN). As such transcoder-free operation (TrFO) is possible, which results in much better voice quality. This feature is part of release 4.
- Addition of an IP-based multimedia subsystem (IMS) that introduces the capabilities to support IP-based multimedia services, such as voice over IP (VoIP) and multimedia over IP (MMoIP), and makes use of the packet-switched network for the transport of control and user plane data. The PS domain also deals with all the mobility (handover) aspects. This feature is part of release 5.
- Introduction of IP transport technology within the UTRAN, as an alternative to the ATM-based UTRAN. This feature is also part of release 5.

It is important to stress that these evolutions are independent of each other and can also be deployed in a fully independent way. This means that for each of these evolutions the operator can make an independent yes/no decision. The later evolution steps are:

IMS — The introduction of the IMS system is driven by the demand to offer more and enhanced services to end-users. It is clear that IP plays a major role in the quick introduction of new services. Operators are faced with the challenge of finding their role in these new business opportunities. Based on their specific strengths such as expertise in communication and powerful billing systems, network operators are now moving into communication-oriented services. To do this, network infrastructures must be transformed into secure, open, and flexible platforms on which third-party developers and service providers can add rapidly and cost effectively generic as well as customized applications.

The main drivers leading this transformation of the value model of the public telecom market can be analysed along three directions:

- **Provision of user-centric solutions**: Market demand for services are evolving from a standardized "one-size-fit-all" service offer to a fully customized service offer that adapts to the user's choice and preference, as well as terminal and location.
- **Usage of the new capabilities of networks and terminals**: Available bandwidth is increasing, which enables the deployment of media-rich services making use of all capabilities for interactivity. Control capability for network resources is enabling provision of the adapted media to the user with the expected levels of quality of service (QoS) and security.
- **Evolution of marketplace and business**: With the shift in value chain, new roles are defined and new stakeholders taking their place in the market (service provider, service retailer, etc.). In parallel, deregulation and the need for timely coping with fierce competition fuel openness toward third parties and support for open service creation and provision.

3GPP has selected the SIP protocol as the only call control protocol between terminals and the mobile network. Interworking with other H.323 terminals (e.g., fixed H.323 hosts) will be performed by a dedicated server outside the PLMN. 3GPP also decided to use IPv6 as the only IP version for the IMS components.

Figure 7.7 shows [7] the proposed 3GPP all-IP UMTS core network architecture [16]. New elements in this architecture are:

- **Call state control function (CSCF)**: The CSCF is a SIP server that provides/controls multimedia services for packet-switched (IP) terminals, both mobile and fixed.
- **Media gateway (MG)**: All calls coming from the PSTN are translated to VoIP calls for transport in the UMTS core network. This media gateway is controlled by the MGCF using the H.248 protocol.
- **Media gateway control function (MGCF)**: The first task of the MGCF is to control the media gateways via the Media Gateway Control Protocol H.248. Also, the MGCF performs translation at the call control signalling level between ISUP signalling, used in the PSTN, and SIP signalling, used in the UMTS multimedia domain.
- **Home subscriber server (HSS)**: The HSS is the extension of the HLR database with subscribers' multimedia profile data.

7.3.2.1 IP-Based UTRAN

The reference architecture for such an IP-based UTRAN is shown in Figure 7.8. The transport mechanism in the release 3 UTRAN is based on ATM/ATM adaptation layer 2 (AAL2). The IP network that interconnects node B and RNC can be owned by the mobile operator, but can also make use of another carrier's IP network. The IP transport network itself now performs the concentration function of the RNC. Some technical challenges that had to be dealt with are related to QoS (due to short delay requirements in the RAN), efficiency in the last mile, and so on [4, 5]. It is more flexible in the mapping between node B and RNC servers and makes more efficient usage of transport resources. It reuses the existing transmission (layer 2 independence); IP can be supported by transmission equipment used today for GSM and UMTS.

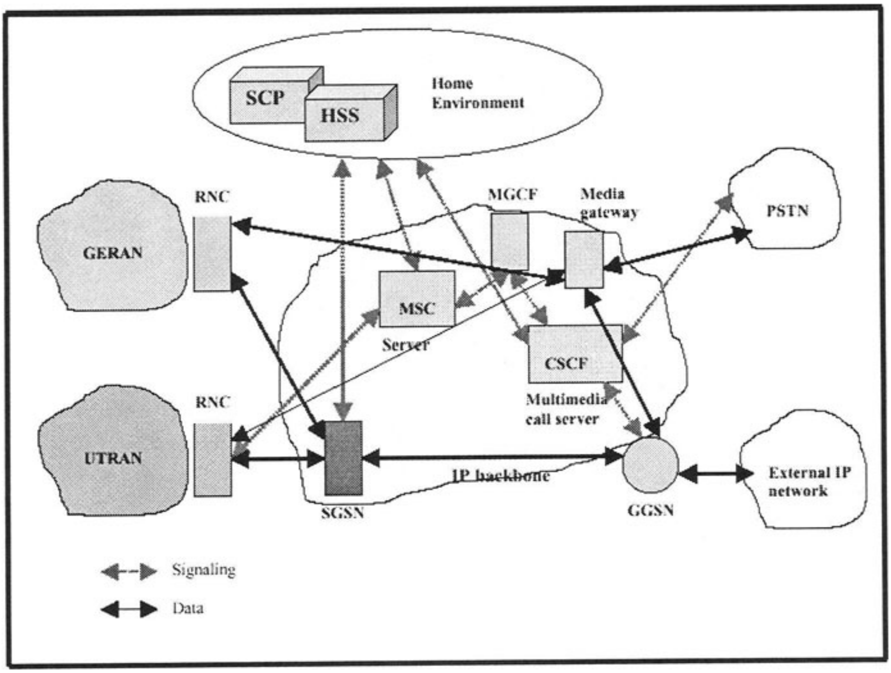


Figure 7.7 3GPP All-IP Architecture

Apart from the pure replacement of transport technology toward IP, it also enables other evolutions in a smooth way. The first additional evolution is to evolve from a pure hierarchical architecture as we have today in UMTS release 3 toward a distributed architecture, which allows, for example, a direct connection from serving RNC to node B, avoiding passing through the drift RNC. IP also enables easier evolution toward NGN architecture within the RAN, where control plane functions are physically separated from user plane functions, which allows for improved scalability and flexibility features.

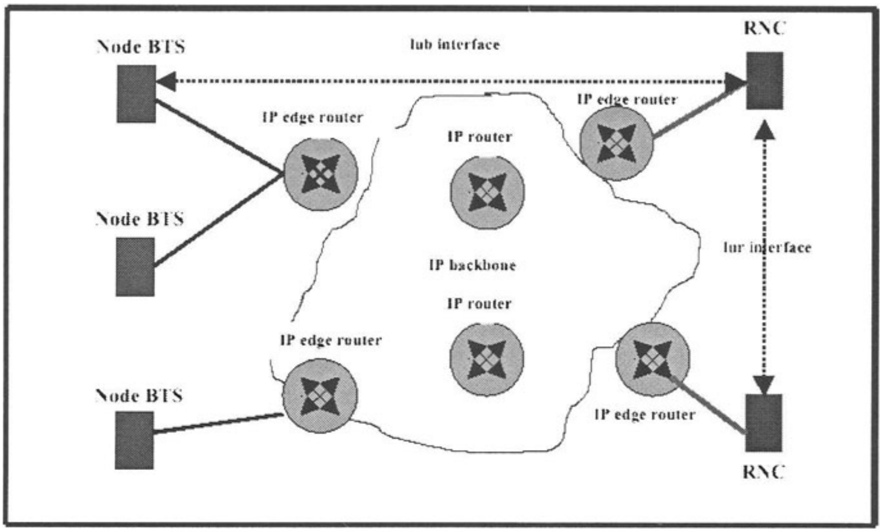


Figure 7.8 IP-bsaed UTRAN

7.3.3 CDMA2000 Network Architecture

The basic architecture is quite similar to the GSM/UMTS architecture. The network architecture for a cdma2000 network (defined in 3GPP2) is shown in Figure 7.9 [7]. The main differences with the GSM/UMTS architecture are in the packet domain where a packet data switching node (PDSN) is used. It has a similar role to the SGSN and GGSN in UMTS. Mobility management within 3GPP2, however, is based on Mobile IP (RFC2002) instead of GPRS mobility management in GSM/UMTS PS networks. Further-more, ANSI-41 MAP signalling is used instead of GSM MAP signalling. Activities have started in 3GPP2 for evolution toward an all-IP network, similar to the IMS activities in 3GPP.

7.4 INTER-TECHNOLOGY ASPECTS

In parallel to the wide-area cellular mobile services, several access technologies are available and can be grouped in the following categories [10]:

- Cellular mobile radio systems
- Cordless systems (e.g., DECT)

- Systems for short-range connectivity such as Bluetooth and the DECT data system
- WLAN-type systems such as ETSI BRAN HIPERLAN 2 and HIPERACCESS, and IEEE 802.11a
- Fixed wireless access or wireless local loop systems
- Satellite systems
- Broadcasting systems such as DAB and DVB-T
- Cable systems such as xDSL over twisted pair and cable modems using transmission over coaxial cables (e.g., CATV systems)

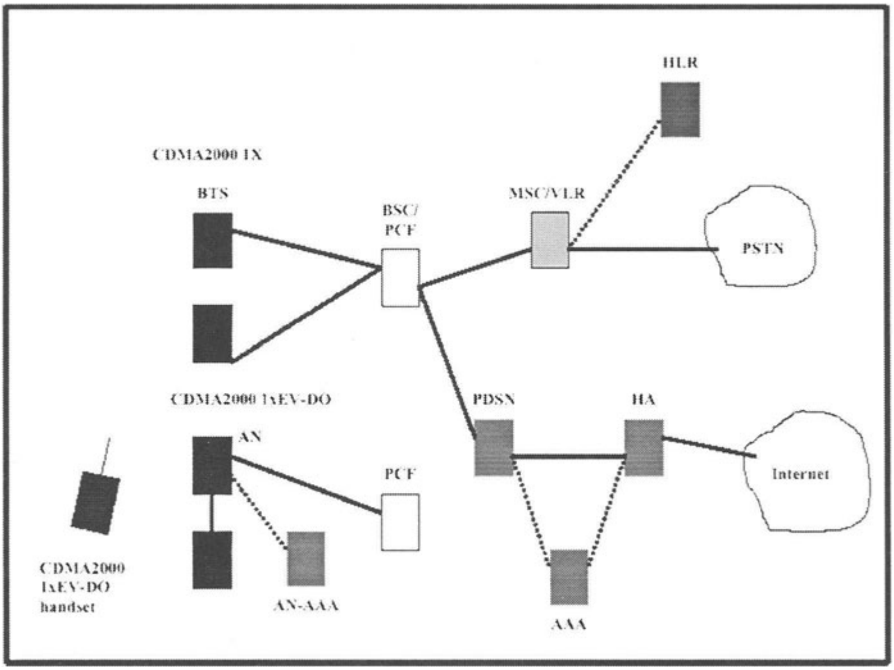


Figure 7.9 cdma2000 1x and cdma2000 1xEV-DO network

The WLAN-type systems are designed in particular for high-data-rate access and low range, and in general for low mobility. They are applicable to corporate networks and public access as a complement to cellular mobile radio systems (e.g., GSM and UMTS, cdma2000) for hot spot applications such as company campuses, conference centers, airports, hotels, and railway stations. The physical layer of the ETSI BRAN system HIPERLAN2 is harmonized with IEEE 802.11a and MMAC in Japan, which would basically allow global roaming.

In addition to these evolving and emerging radio access technologies, research on a new radio interface is proposed, especially in Japan, which should support high mobility and high data rates. Ad hoc or self-organizing networks will play a complementary role to extend coverage for low-power systems and unlicensed applications. In these systems mobile stations may act as relay stations in a multihop transmission environment from distant mobiles to base stations.

Mobile stations will have the ability to support base station functionality. Direct mobile-to-mobile calls will be possible. The network organization will be based on interference measurements by all mobiles and base stations for automatic and dynamic network organization according to the actual interference and channel assignment situation for the channel allocation of new connections and link optimization.

Fixed wireless access or wireless local loop systems are developed to replace or complement wired access systems. These systems do not support mobility. DAB and DVB-T can be applied to wideband broadcast data services in the downlink.

These systems can be combined with cellular mobile radio systems like GSM and UMTS or the public switched telephone network (PSTN) and integrated services digital network (ISDN) for the uplink as a return channel for user requests and highly asymmetrical services. Fixed lines based on copper twisted pair or coaxial cables are widely distributed. Coaxial cables support high bandwidth and could be used for wideband data services. The potential of twisted pairs is used by ISDN and xDSL techniques (mainly ADSL) [1, 2,17]. These technologies represent a very flexible and powerful platform to support future requirements of services and applications in pervasive networking infrastructure. However, most of these systems have been designed in isolation without taking into account possible interworking with other access technologies.

7.4.1 WLAN

Independent development of WLAN standards in the European Telecommunications Standards Institute (ETSI) and the IEEE has produced multiple noncompatible WLAN air interface standards. These operate on 2.4 GHz and 5 GHz uncoordinated industrial, scientific, and medical (ISM) hands. The dominant access method at the moment is the IEEE 802.1lb standard with 11 Mb/s air interface rate on which this article concentrates [17].

7.4.1.1 The IEEE 802.11 Standard

The IEEE *802.11* standard [18] offers several wireless LAN technologies for use in the unlicensed 2.4 and 5 GHz bands. Legacy 802.11 systems operate in the 2.4 GHz band with three different PHY layers sharing the same MAC layer. These PHY layer specifications are the seldom-used infrared (IR) technology, and the more popular direct-sequence spread spectrum (DSSS) and frequency hopping spread spectrum (FHSS) systems achieving 1 and 2 Mb/s data rates. Operating under the same 802.11 MAC layer in the 2.4 GHz band, higher data rates are supported by the IEEE 802.11b PHY layer specification using complementary code keying (CCK) modulation achieving data rates of 5.5 and 11 Mb/s. Recently, a new task group, IEEE 802.11g, has been formed to draft a standard that achieves data rates higher than 22 Mb/s. Alternatively, in the 5 GHz band, the IEEE 802.11 standard offers the 802.11a specification that uses orthogonal frequency-division multiplexing (OFDM) achieving data rates up to 54 Mb/s. A new task group, 802.11e, has been created to accommodate additional QoS provisions and security requirements at the MAC layer while supporting all of the previously mentioned legacy 802.11 PHY layers.

The IEEE 802.11e group is now tasked with creating a new 802.11 MAC protocol by adding on top of the legacy 802.11 MAC layer specification. The proposed 802.11e additions do not include guaranteed QoS in the ad hoc connection mode, which is paramount for high-rate WPAN applications. Some form of QoS will be available in the coordinated network mode. Even at the completion of the new 802.11e MAC specification, the legacy burden for LAN functionality and the requirement to support numerous PHY layers will likely render the MAC implementations too complex and power-inefficient for the high-rate WPAN applications.

From a PHY layer point of view, the IEEE 802.11b specification supports data rates up to 11 Mb/s. The newly formed task group, IEEE 802.11g, contemplates support for data rates higher than 22 Mb/s. Two leading PHY layer candidates for the 802.11g standard are single-carrier trellis-coded & phase shift keying (PSK) modulation and OFDM schemes. Both candidates offer considerably more costly radio and baseband implementations than the 802.15.3 PHY layer. The approval of the 802.11g specification requires an FCC rule change in the FCC Part 15.247 rules, for which a Notice for Proposed Rule Making (NPRM) process is underway. Finally, the 802.11a technology operating in the unlicensed 5 GHz band supports data rates up to 54 Mb/s.

7.4.1.2 Bluetooth Wireless Technology

The specifications of Bluetooth [19] are maintained and developed by the Bluetooth Special Interest Group (SIG). Bluetooth was initially targeted as a replacement for cable or infrared connectivity. Expanded visions now include many different kinds of applications, from dial-up networking to LAN access and ad hoc networking, from data base synchronization to personal area networks.

Bluetooth radios operate in the 2.4 GHz license-free ISM bands and support symmetric and asymmetric links. Synchronous symmetric channels are intended for 64 kb/s continuous voice traffic. The asynchronous connectionless (ACL) channel can support 723.2 kb/s asymmetric data rate with 57.6 kb/s in the return direction or 433.9 kb/s symmetric data rates. Due to the Bluetooth SIG license agreement, the development of the specification is not made available to the general public until it is finished and approved by the Bluetooth SIG. Adopter members have the privilege to look at the specification prior to its public availability. The Bluetooth specification, currently at version 1.1, comprised the following two parts:

The core specification defining the radio characteristics and the communication protocols for exchanging data between devices over Bluetooth radio links.

The profile specification that defines how the Bluetooth protocols are to be used to realize a number of selected applications.

In July 1999, the Bluetooth SIG submitted the just created Bluetooth specification as a candidate for an IEEE 802.15 standard. The Bluetooth proposal was chosen to serve as the baseline of the 802.15.1 standard. As of this writing, the development of the draft standard is in its final stages, having successfully completed two sponsor ballots. In addition to the IEEE 802.15.1 activity, the IEEE 802.15.2 task group studies coexistence issues between 802 wireless technologies. The 802.15.3 task group is developing standards for high-rate radios (>20 Mb/s). Finally, the 802.15.4 task group is developing standards for low-rate radios (<200 kb/s).

7.4.1.3 IEEE 802.15.3 Wireless PAN Standard

The 802.15.3 MAC layer specification is designed from the ground up to support ad hoc networking, multimedia QoS provisions, and power management. In an ad hoc network, devices can assume either master or slave functionality based on existing network conditions. Devices in an adhoc network can join or leave an existing network without complicated setup procedures. The 802.15.3 MAC specification provides provisions for supporting multimedia *QoS*. MAC superframe structure consists of a network beacon interval, a contention access period (CAP), and a contention-free period (CFP) reserved for guaranteed time slots (GTS). The boundary between the *CAE'* and GTS periods is dynamically adjustable. The 802.15.3 PHY layer operates in the unlicensed frequency band between 2.4 GHz and 2.4835 GHz, and is designed to achieve data rates of 11-55 Mb/s that are commensurate with the distribution of high-definition video and high-fidelity audio. The 802.15.3 systems employ the same symbol rate, 11 Mbaud, as used in the 802.11b systems. The 802.15.3 signals occupy a bandwidth of 15 MHz, which allows for up to four fixed channels in the unlicensed 2.4 GHz band. The transmit power level complies with the FCC 15.249 rules with a target value of 0 dBm. The RF and baseband processors used in the 802.15.3 PHY layer implementations are optimised for short-range transmission limited to 10 m [20].

7.4.1.4 ETSI HiperLAN2

HiperLAN2 operates in the unlicensed 5 GHz band offering an actual throughput around 40 Mb/s, superior to IEEE 802.11a. Hiper-LAN2 solves many issues associated with 802.11a, in particular interference, security, and QoS. A convergence of 802.11a and HiperLAN2 technologies would be beneficial by providing a clear market focus in the 5 GHz band similar to what has been accomplished in the 2.4 GHz band. This initiative was launched recently between IEEE and ETSI, and the harmonization effort has already been made. This standard also relies on the OFDM modulation to reach a good performance in highly dispersive channels. The transmitted symbols are mapped onto multiple (48) subcarriers, and in parallel pilot tones are sent to facilitate tracking. HiperLAN2's main differences are the dynamic frequency selection (DFS) process, which automatically assigns the carrier frequency according to interference measurements, and the scheduling algorithm that grants resources to connections with respect to the connection type [7].

7.4.1.5 Summary of Key Features

Table 3 summarizes the key features of the standards IEEE 802.11.3, IEEE 802.11a,b, ETSI HiperLAN2 and Bluetooth [10] [20].

7.4.2 Wireless Local Loop (WLL)

Wireless local loop (WLL) is providing service to densely populated urban areas, as well as sparsely populated remote and rural areas [21]. The emphasis of WLL is service to fixed terminals; mobility is also an advantageous feature. In recent years a number of manufacturers have developed nonstandardized systems specifically designed for WLL applications. The ITU has provided recommendations on implementation of WLL systems based on common cellular mobile radio standard Digital Enhanced Cordless Telecommunications (DECT), Personal Access Communication System (PACS), and Personal Access Communication System (PACS) are three well-known international standards for low-mobility low-power wireless communication applications [22]. These standards have been developed for operation in microcellular environments with small cells, typically several hundred meters in diameter. However, with fixed elevated antennas at subscriber locations, and other enhancements and modifications, the range can be extended to several kilometres, making them suitable for WLL applications in sparsely populated areas.

Table 7.3 Key features of different standards

	Bluetooth	IEEE 802.15.3	IEEE 802.11.b	IEEE 802.11.a	ETSI Hiper LAN2
Frequency Brand (GHz)	2.4	2.4	2.4	5	5
Data Rate (Mb/s)	< 1	Up to 55	5.5	30	40
Typical Range (m)	~5-10	10	50-100	50-100	50 (indoor)/300 (outdoor)
Medium Access Control	TDD	CSMA/CA	CSMA/CA	CSMA/CA	TDD
Modulation	GFSK	QPSK	CCK	OFDM	OFDM
QoS Support	SCO	Guaranteed Time Slots	PCF	PCF	FCA, FSA
Handover Support	No	No	No	No	Yes
Radio Link Quality Control	No	Link Adaptation	Link Adaptation	Link Adaptation	Link Adaptation
Fixed Network Support	RS-232, TCP/IP	Ethernet	Ethernet	Ethernet	Ethernet, ATM, IEEE 1394
Availability	Now	Now	Now	Now	Now

7.4.2.1 Overview of Three Standards

7.4.2.1.1 DECT

DECT is a European standard developed by the European Telecommunications Standards Institute (ETSI) [23] [24]. It is designed to operate in the 1880–1900 MHz frequency band, with flexibility to use other close bands. It is based on TDMA-time-division duplex (TDD) principles. The number of carriers is 10, and carrier separation is 1726 kHz. Transmission rate is 1152 kb/s, and the number of TDMA channels for each carrier is 12. Therefore, the total number of voice channels is 120 (10 carriers · 12 time slots/carrier). Speech coding is 32 kb/s ADPCM, and the modulation method is Gaussian frequency shift keying (GFSK). Channel assignment is dynamic. Normal cell radius in DECT is several hundred meters.

7.4.2.1.2 PACS

PACS was developed in the United States and standardized by the Joint Technical Committee (JTC) in 1994. It operates in two wide duplex bands, 1850–1910 MHz (uplink), and 1930–1990 MHz (downlink). These bands were allocated by the FCC in three paired 5 MHz and three paired 15 MHz bands for licensed wideband personal communications services (PCS) applications. Also, a 10 MHz band (1920–1930 MHz) has been allocated for unlicensed TDD operation. The air interface of PACS allows FDD operation in the licensed band and TDD operation in the unlicensed band [4]. The PACS standard is based on FDD-TDMA with 200 channels (carrier separation of 300 kHz). Modulation and speech coding are $\pi/4$-QPSK (quadrature phase shift keying) and 32 kb/s ADPCM, respectively. Bit rate per channel is 384 kb/s. Channel assignment is quasi-static autonomous frequency assignment dynamic channel assignment (QSAFA/DCA) [25] [26]. The standard is designed for low-mobility applications.

7.4.2.1.3 PHS

PHS is the Japanese-developed standard operating in the 1895–1918 MHz band. PHS was envisioned as an efficient low-cost cordless and portable phone system. In late 1993, the Research and Development Centre for Radio Systems (RCR), currently known as the Association of Radio Industries and Businesses (ARIB), approved the RCR STD-28 standard. The Telecommunication Technology Committee (TTC) subsequently completed the interface for connection to the network, and trial systems started operation. The first commercial system was implemented in mid-1995. PHS is based on TDMA-TDD principles with 77 channels (carrier separation of

300 kHz). The bit rate is also 384 kb/s, and modulation is π/4QPSK. Speech coding is 32 kb/s ADPCM, and channel assignment is dynamic. Each physical channel can be used as four traffic channels in TDMA mode [27].

7.5 SEAMLESS PERVNET ARCHITECTURE

Third-generation mobile radio systems for mobile multimedia applications have been deployed by 2001 and 2002 in different regions. Due to the long necessary timeframe for the definition, development, and standardization of new systems beyond third-generation mobile radio systems along with the match of the requirements in running different applications in PervNet (refer to Chapter 2 for details) environment, discussions are already starting today.

What are the motivations for further developments for the PervNet environment?

Frequency spectrum is scarce resource, which requires more efficient use of spectrum and the exploration of new frequency bands for pervasive applications.

Increasing computing power at lower cost enables new possibilities for more sophisticated signal processing algorithms for, say, coding, decoding, detection, advanced antenna concepts, and software-defined radio implementations.

Different flexible and broadband access technologies are evolving and emerging, which are optimised for special purposes. Their integration in a common flexible and expandable platform would provide a multiplicity of possibilities for current and future services and applications to users in a single terminal.

User expectations are increasing more sophisticated services with QoS comparable to wireline access based on the current development in the Internet.

The major driving forces for PervNet environment will support user demands for new and advanced services with high security and privacy, *minimal user distraction and localize scalability*

Figure 7.10 shows [7] this vision of a seamless PervNet (based on the core model depicted in Figure 2.2) including a variety of interworking access systems, which are connected to a common IP-based core network. The media access system connects each access system to a common core network. Due to the different application areas, cell ranges, and radio environments, the different access systems are organized in a layered structure according to the structure given in Chapter 2. Here, the access layer is magnified in different sublayers (Figure 7. 11) [10]. However, in addition to different cell layers, different access technologies also complement each other on a common platform in pervasive network environment.

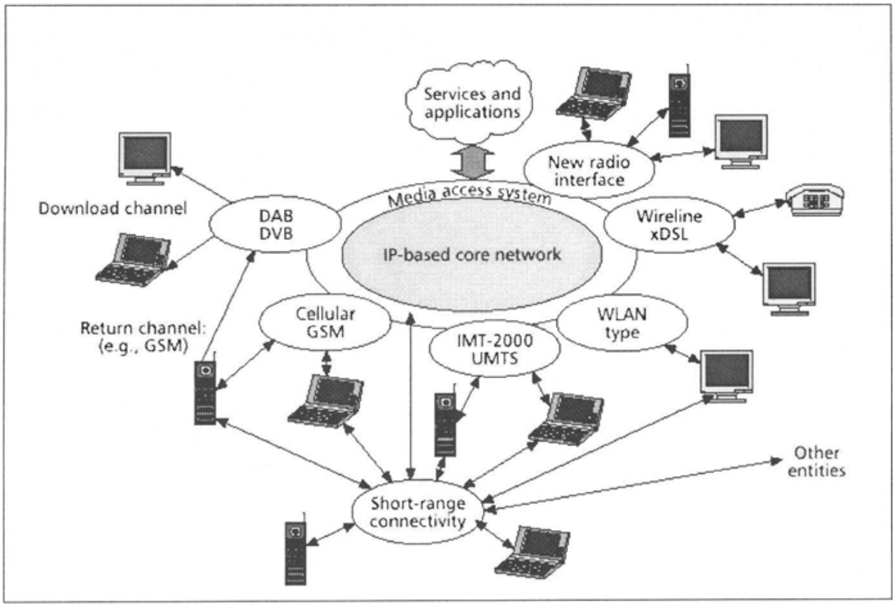


Figure 7.10 Seamless PervNet Architecture

- **Cellular layer** for full coverage, multimedia, medium-bit-rate applications. This is the area of GSM, CDMA, or UMTS mobile networks.
- **Hot spot layer** for high bit rates in a short-range local mobility environment. This is the area of WLAN networks.
- **Personal network layer** provides a short range of interconnectivity between different equipment (printers, PDAs, home appliances, etc.). Interconnection of this equipment to the other layers of communications via multi-mode terminals is the area of Bluetooth. The transparent delivery of services across these network layers in an optimum way will require a dynamic bandwidth management function operating on diverse wireless technologies while maintaining a continuous session. This new media access layer will connect the access networks to the core network while ensuring mobility management, security, and QoS. The ETSI Broadband Radio Access Network (BRAN) standardization body investigates, for HiperLAN2, two approaches for interconnection of WLAN and UMTS networks:

A tight coupling scheme, to offer a seamless handover and the same level of security in WLAN and UMTS networks. This approach would require a simplified Iu interface for interconnection of WLAN network to UMTS core network.

A loose coupling scheme, which would rely on IP protocols to organize mobility and roaming between access networks. Interworking between WLAN and the core network is performed between the authentication, authorization, and accounting server (AAA) and the home location register (HLR).

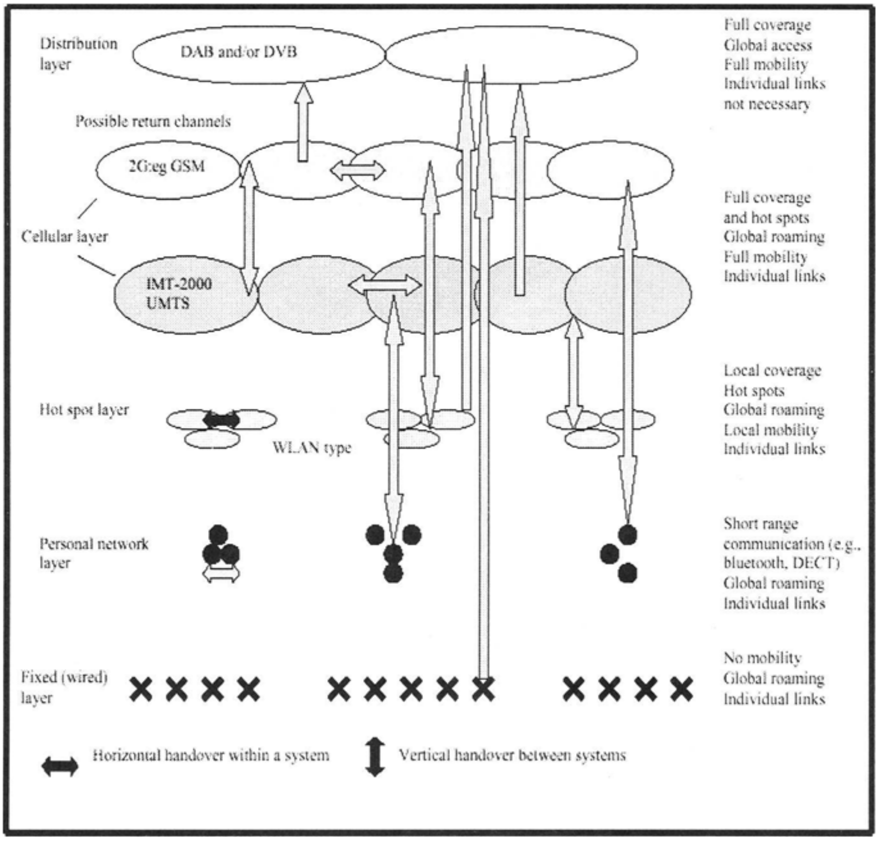


Figure 7.11 Access sublayer of seamless PervNet

•Distribution layer: Due to the big possible range and cell size of DAB and DVB-T, these systems are especially suited to distribution or broadcast services.

•Fixed (wired) layer: Fixed access systems are twisted pair systems (xDSL) and coaxial cable systems (e.g., CATV). Fixed wireless access or wireless local loops can be placed in this category. Fixed access systems do not support mobility.

7.6 FUTURE DIRECTION

Many technical challenges must be solved by extensive research to make the vision of systems beyond the third generation happen. The key points are the interworking of different access systems on a common platform and the necessary multimode or adaptive and multiband terminals for different access systems and a wide range of services. Challenges are in several areas, such as the radio interface, the radio access and core network, implementation issues, and services-related issues.

2G mobile communications has brought about a revolution in ways of living. And the revolution is not over, with mobile Internet and 3G services being offered in coming years. Through an evolution of technology, new services have been or will be offered to subscribers. UMTS and its evolutions will provide even higher data rates, and a more comfortable offering of more demanding services. The evolution from 2G toward 3G will also lead to more convergence through a reduction of the number of main 3G cellular technologies. In the short to mid-term, interworking with WLAN is envisioned, as well as the offering of multimedia (including real-time) services via the IMS system. Even all this will not be the end of the evolution of mobile communications as activities are ongoing within the research community on topics beyond 3G (e.g., satellite component of UMTS, Mobile Broadband System at 60 GHz) i.e., to develop a PervNet environment.

REFERENCE

[1] Otsu T., et.al. Network architecture for mobile communications systems beyond IMT-2000. IEEE Personal Communication Services Oct 2001; 31-37

[2] Frodigh M. Future-generation wireless networks. IEEE Personal Communication Services Oct 2001; 10-17

[3] ARIB. MMAC. http:// www.arib.or.jp/mmac

[4] ETSI. HiperLAN2 Standard. http://www.etsi.org

[5] Abeta S. et.al. Coherent DS-CDMA and MC-CDMA broadband packet wireless access in a multi-cell environment. Proceeding IEEE VTC-2000. Sep 2000

[6] Kojima F., et.al. Adaptive sub-carriers control scheme for OFDM cellular systems. Proceeding VTC 2000. May 2000

[7] Vriendt De Johan. Mobile network evolution: a revolution on the move. IEEE Communications Magazine Apr 2002; 104-11

[8] Chai J and Goodman D.J. General packet radio services in GSM. IEEE Personal Communication Services Oct 1997; 122-31

[9] ETSI. GSM 3.64. May 1997. www.etsi.org

[10] Mohr W., Konhauser W. Access network evolution beyond third generation mobile communications. IEEE Communications Magazine Dec 2000; 122-33

[11] Berruto E., et.al. Research activities on UMTS radio interface, network architectures and planning. . IEEE Communications Magazine Feb 1998; 82-95

[12] Chaudhury P., Mohr W., Onoe S. The 3GPP proposal for IMT-2000. IEEE Communications Magazine Dec 1999; 72-81

[13] ITU-R TG 8/1. Detailed specifications of the radio interfaces of IMT 2000. Doc 8-1/TEMP/275-E, 18th mtg of TG 8/1. 1999. Helsinki, Finland

[14] 3GPP home page: http: \\ www.3GPP.org

[15] 3GPP2 home page: http: \\ www.3GPP2.org

[16] Bos L., Leroy S. Towards an all-IP based UMTS architecture. IEEE Network Jan-Feb 2001; 36-45

[17] Kalliokulju J., et.al. Radio access selection for multistandard terminals. IEEE Communications Magazine Oct 2001; 116-24

[18] IEEE 802.11. Local and metropolitan area networks: wireless LAN medium access (MAC) and physical (PHY) specifications. ISO/IEC 8802-11:1999(E)

[19] Bisdikian C. An overview of the bluetooth wireless technology. IEEE Communications Magazine Dec 2001; 86-94

[20] Karaoguz J. High rate wireless personal area networks. IEEE Communications Magazine Dec 2001; 96-102

[21] ITU-R. Handbook on land mobile (including wireless access) vol. 1: wireless access local loop. 1996

[22] Momtahan O., Hashemi H. A comparative evaluation of DECT, PACS and PHS standards for wireless local loop applications. IEEE Communications Magazine May 2001; 156-63

[23] ETSI Draft ETS 300 175-1. Radio equipment and system (RES): DECT common interface, Part I: overview. 2nd ed 1995

[24] Yu C C., et.al. Low tier wireless local loop systems-Part I: introduction. IEEE Communications Magazine May 1997; 84-92

[25] Noerpel A. R., Lin Y.B., Sherry H. PACS: Personal communications system: a tutorial. IEEE Communications Magazine Jun 1996; 32-43

[26] Chuang J.C.I. Autonomous adaptive frequency assignment for TDMA portable radio systems. IEEE Transaction on Vehicular Technology Aug 1991, 627-35

[27] Suzuka Training Institute. Introduction of personal handy-phone systems. 1995

Chapter 8

Challenges

The design and implementation of PervComp is an ongoing effort. While some progress has been made, there are still a number of major issues to be addressed. We are still many years behind from Weiser's vision [1]. For example, in PervComp, users will work through a wide variety of devices, some with very limited capabilities and they may attach to an ad-hoc proliferation of wired/wireless networked appliances. Although many of these nodes will be acting as routers, they must be entirely plug-and-play (PnP) and must form a network without manual intervention, as much as possible. The way wireless networks and mobile computing applications are developed, deployed and used today does not meet the expectations of the PervNet user community and falls far short of the potential for PervComp. In this chapter, we discuss about the challenges currently standing between the concept and the implementation of PervNet in particular and of PervComp in general.

8.1 INTRODUCTION

PervComp is taking us beyond the desktop, beyond the anytime anywhere computing, to every time everywhere context-aware computing paradigm. People will create knowledge, not data. Information technology has traditionally focused on managing and retrieving explicitly entered data. We will soon be digitizing and archiving a bulk of human activity. It will be an on-going stream culled from everyday human activities and physical phenomena. The analysis, processing and organization of this information must become more automated. Access to information cannot stop because a computer has crashed, a link is stale, or a subset of information is not entirely consistent. The challenge is to develop an architecture [2] that continuously provides service on top of a highly dynamic underlying network of information.

Flexible architectures are loosely organized and adaptive, allowing great confidence in its operation, and providing administrative scalability (i.e., the administration of a complex system on a planetary-scale by multiple, unaffiliated people with unique objectives, while its physical and logical resources are constantly changing). So, when millions of people will be conducting their efforts on-line with shared information, the confluence of their actions becomes a powerful means of enhancing our productivity and extracting knowledge from information. The challenge is to automatically infer relationships among information, delegate control, and establish authority from available information, assisted with new ways to interact with information and people to enhance human productivity. Hence, personal information management will be one of the major *Killer Applications.* Computer usage will be shifting from corporate processing to the management, analysis, aggregation, dissemination, and filtering of information for individuals in all aspects of their lives.

Several non-technical issues will also come in the forefront, apart from the networking and computing issues that are mostly talked about now. Subsequently, there will be implications of PervComp on issues such as social, economical, legal and so on. Unfortunately, we are yet to mature in these areas as an aftermath of the revolution of the Internet (not to speak of PervNet). For example, in many countries, as of today, laws and regulations on the Internet usage (and misuses) are not clearly defined. Hence, it is extremely difficult to even guess at this point the non-technical challenges that will crop up after the full-fledged deployment of PervComp [3].

8.2 PERVNET CHALLENGES

The following discussion will concentrate on the research agenda coming out of the gap between the vision of PervNet, as depicted in Chapter 2, and the current state of the art achieved thus far in networking technology.

8.2.1 Plug-n-Play

As Weiser [1] visioned, in PervNet, devices will enter and exit the network off and on. If the time taken by the devices to make PervNet sense their entry be too long, devices will be unplugged from PervNet before they are configured and allowed to communicate. In fact, devices with embedded computers will appear and disappear from the containing PervNet at a frantic rate. How are their interfaces to be handled? A common vital element in the solutions to these problems is transparency. The devices have to be absolutely plug-n-play. Think of today's PC environment. How often do you buy a new computer? Once in a year. And when you do, how long does it take to get it set up the way you need it? One hour or so. Rather than acquire a new computer every year, if you acquire them every minute, how much time should it take to be configured? Certainly, less than a second. When every manufactured product you see larger than a paper clip is a computer, how do you configure them? All these challenges are to be coped up with in PervNet deployment. Similarly, the development of low cost network interfaces and their integration into everyday appliances is also an active area of investigation and development.

8.2.2 Scalability

The first wave of pervasive devices with a network interface will extend PervNet to trillions of devices. This is expected and probably manageable. But it is the second wave, the instrumentation of non-electronic devices, which ushers in the true PervComp environment, will be too difficult to tackle unless the underlying PervNet is designed to be perfectly scalable. However, given the scenario of PervNet architecture (vide Chapter 2), scalability in PervNet management will be a complicated issue no doubt. When every book, packet, street sign, soda can and pen is active and networked, the number and diversity of devices challenge our ability to control and manage them. Building robust lookup services that support discovery and scaling are still a major focus. While finding a service from a list of hundred services is easy, building a system that can handle thousands of services continuously is not that easy. Moreover, updating their availability is a prerequisite to wide spread deployment of intelligent environments.

8.2.3 Extensibility

For an ad hoc dynamic heterogeneous global network like PervNet, extensibility must be elastic in order to support the PervComp environment. Otherwise, it will loose its pervasive nature; there will remain isolated islands of disconnected networks. For instance, as it expands for a typical user moving from a single room to multiple rooms and hallways, several new challenges appear. One geometric model may no longer suffice. Vision and other perception systems will need to cooperate and hand-off tracks of users between different disjoint spaces. Currently, it is unclear how services span boundaries between spaces or how these extents might be affected by dynamic network partitioning and regrouping.

8.2.4 Protocols

Although backbone network protocols are maturing fast (such as IP over WDM as discussed in Chapter 6), mobile wireless network protocols are bottlenecked by a number of obscurities and controversies (such as mobile IP versus IPv6). Design of wireless network protocols is still an area of active research work. In particular, issues of mobile users and the equivalent of the "Slashdot Effect" [4], where millions of consumers want access to a single message stream, present extreme challenges to the routing infrastructure. Moreover, as a whole, the architecture of PervNet is not put to consensus at any level. This is very vital because nobody wants the history of OSI model to be repeated here too. Since there are various propositions of PervNet (one such model is proposed in this book in Chapter 2), convergence to a single effective model of implementation is a prerequisite for success of PervComp. For instance, how to interconnect millions of subnets? Heterogeneity requires protocol converters at every interface between disparate networks. How to put these converters at suitable interface points and how to make them scalable? Similarly, addressing (discussed in Chapter 7) is a big issue while designing routing protocols, which should have the advantage in scalability. Transport protocols (such as TCP) have to handle congestion more efficiently. Will the existing protocol stacks suffice? If not, how to synthesize the new protocols, keeping the constraints of PervNet in mind?

8.2.5 Security

Wireless network security is only at its infancy. Even security of public wired network is not mature enough to convince users to type in their credit card numbers (say, over the Internet). In the circumstances, it is easy to imagine the challenge that lies ahead in implementing a secure PervNet. The basic requirements for securing PervNet communications are simple: firstly to prevent unauthorized subscribers from receiving messages, and secondly to prevent attackers from "spoofing" messages from a legitimate producer. The possibility for eavesdropping and losing sensitive information becomes overwhelming once computers are disposable. The volume of data available about you and your life in PervComp becomes absolutely staggering. How do we secure your information environment whilst retaining the availability and mobility of your data? How do we balance the benefits of availability whilst protecting against intrusion?

Privacy of both the authorization keys and message content can be preserved by encryption of the link between the client library and the server. Users can specify their preference for security mechanism, authentication and privacy during connection establishment. The use of authentication and privacy is optional, and computationally expensive. The major problem with this mechanism is that the plaintext of the messages, is exposed to the intermediate servers routing the message to its destinations. Unfortunately, when using the content to perform the routing, this is unavoidable. Of course, it is always possible to encrypt the body of the message prior to transmission if required.

8.2.6 Quality of Service (QoS)

Applications running over PervNet must support end-to-end quality of service (QoS) for users and developers, for example, in terms of performance, availability, maintainability, and survivability. The information-driven applications, using PervNet as underlying communications infrastructure, will do the computation of the QoS properties supported by an end-to-end connection in PervNet, calculated from the QoS properties of the component links. PervNet should support information flow through a variety of environments with these QoS properties. As discussed in Chapter 2, PervNet includes high-speed networks, such as the Next Generation Internet, on one end of spectrum, and limited bandwidth wireless connections on the other end. The wireless portion that interconnects mobile hosts/routers can change rapidly in unpredictable ways or remain relatively static over long periods of time. These bandwidth constrained wireless networks typically support best effort voice and data communications, where the achieved "goodput" is often lower than the maximum radio transmission rate after encountering the effects of multiple access, fading, noise, and interference, etc. In addition to being bandwidth constrained, components of PervNet may be power-constrained too because pervasive devices mostly rely on battery power for energy. These environments are also characterized by continuous topology changes that demand stable and responsive system level adaptation. PervNet has to support the information flow through these changing environments. Thus, providing suitable QoS support for the delivery of real-time audio, video and data in PervNet represents a number of significant technical challenges. It needs a suitable QoS framework paying particular attention to the performance of the signalling system under a variety of network, mobility and traffic conditions in support of fast reservation, restoration and adaptation. The system will manage resources according to the user-specified QoS declarations and compete for these resources. It may be assisted by systems software tools supporting broad-sense QoS using adaptive resource management techniques.

8.2.7 Power (Energy)

It is clear by now that building PervNet poses a significant technical challenge because of the many constraints imposed by the environment. The devices used must be lightweight. Furthermore, since they are battery operated, they need to be energy conserving so that battery life is maximized. Several technologies are being developed to achieve these goals by targeting specific components of the computer and optimizing their energy consumption. For instance, low-power displays, algorithms to reduce power consumption of disk drives, low-power I/O devices such as cameras, etc. all contribute to overall energy savings. Other related work includes the development of low-power CPUs (such as those used in lap-tops) and high-capacity batteries. Recent focus has been on developing strategies for reducing the energy consumption of the communication subsystem and increasing the life of the nodes. Power aware routing protocols are aiming to this goal because studies have stressed the need for designing protocols to ensure longer battery life.

8.2.8 Charging

While we anticipate that most use of PervNet services will be "local" and remain uncharged, the provision of information services and federation of PervNet domains requires a charging model allowing producers to add a premium to the basic transportation costs and backbone routers to allocate forwarding costs to users. To complicate matters, the cost of routing is not consistent, and complex subscriptions consume significant CPU resources during evaluation. While a simple model of charging by number of bytes is attractive, it does not allow for accurate cost recovery. Additionally, it is not clear that a single charging model will suffice: allocation of the total cost between the producer and consumers of a service could occur in any number of ways, with neither producer only nor consumers only acceptable. Note that billing is a part of the problem. Servers must simply log the data required for billing which can be processed by a third party. Though simple charging mechanisms are available, charging in a wide-area PervNet remains an open issue. Additionally, think of the following scenario in PervComp. When you throw you lunch wrapper in the trash, its computer negotiates with the trashcan to be recycled or shredded or composted. But your lunch wrapper was bought using your debit account, and the trash can wants to charge you for burdening it with non-recyclable plastic.

8.3 PERVWARE CHALLENGES

8.3.1 Interfaces

As mentioned in Chapter 5, presenting the available services to an user in an understandable fashion and letting the user create and edit automatic behaviors are both on going work items. Current prototypes (e.g., EasyLiving system) can handle a single room and 10's of devices with dynamic changes to their configuration. One to three people can simultaneously use the facility. But, in PervComp scale, user interface issues are to be more rigorously examined. As PervComp evolves, it is expected that input and output devices will no longer be tied to a single machine or application but rather be able to flexibly support user interaction across a wide variety of tasks and modalities. Future work will build on this architecture, further exploring the interface design to accommodate migration of computing from the desktop into everyday living.

8.3.2 Component Interaction

To gain leverage from the substantial work carried out in the distributed systems community, future components of PervComp systems must clearly follow the same basic principles as open distributed systems. They should be designed and implemented in an open and extensible manner, letting us combine components to form applications unforeseen at the time of their deployment. Technically, this implies obvious features such as open interfaces and support for inter-component communication. However, deployed PervComp systems will require assurances from their components in terms of metrics such as performance, security, and reliability. Furthermore, the characteristics of PervComp environments place demands on existing platforms that the platforms have not been designed to address. For example, many existing platforms perform poorly when applied to the type of saturated computing environments described by Weiser [1].

8.3.3 Adaptation

Adaptation is the ability to absorb perturbations in the environment that is subject to change. Such changes might be prompted by variations in resource availability as a result of failures or the deployment of new services or by variations in patterns of usage or mobility. The importance of adaptation is well understood in the field of mobile computing. However, in the environment wherein PervComp components function, it is significantly more complicated, where there is a need to respond to a much larger set of contextual triggers. At a component level, components will be required to adapt internally. More importantly, we might also have to substantially reconfigure applications involving multiple components. The need to manage these configuration changes in ad hoc environments poses significant problems. One recent approach to addressing these problems is to use reflective middleware platforms [2]. Although researchers have generally focused on using reflection to support adaptation in mobile environments, its application to PervComp systems is not an obvious extension.

8.4 PERVCOMP CHALLENGES

8.4.1 Perception

For proactivity to be effective, it is crucial that PervComp tracks user intent and there is of some form of intelligence working on the user's behalf to coordinate the actions of components in the infrastructure. Otherwise, it will be almost impossible to determine which system actions will help rather than hinder the user. Two areas in which this is particularly evident are the system's ability to accurately determine a user's task and intention and its ability to develop associations between components to assist the user in these activities. For example, suppose a user is viewing video over a network connection whose bandwidth suddenly drops [2]. Should the system (a) reduce the fidelity of the video, (b) pause briefly to find another higher-bandwidth connection, or (c) advise the user that the task can no longer be accomplished? The correct choice will depend on what the user is trying to accomplish. Achieving these objectives in anything other than extremely limited domains is an unsolved problem. In PervComp where computing merges with human, this issue has other angles to look at too. From a personal perspective, proactive computing pushes us towards systems that can monitor and handle our bodies directly. Today's systems are poor at capturing and exploiting user intent. On the one hand are generic applications that have no idea what the user is attempting to do, and can therefore offer little support for adaptation and proactivity. On the other hand are applications that try to anticipate user intent but do so very badly.

The need to capture user intent generates a number of important research questions [2]: Can user intent be inferred, or does it have to be explicitly provided? In the latter case, is it statically specified (from a file, for example) or obtained on demand through dynamic interactions? How is user intent represented internally? For example, automatic diabetes regulators (used as wrist bands or belts) require the ability to both monitor blood glucose levels and administer insulin. But a user may not want the insulin to be pushed at a particular moment when he/she is going to take some sugar cubes in coffee very shortly. How rich must this information be for it to be useful? When and how is it updated? Will the attempt to obtain intent place an undue burden on the user? Will it hurt usability and performance unacceptably? A system such as this would still require significant advances in software reliability to be feasible. How do different layers of a system access this knowledge? How does one characterize accuracy of knowledge in this area? A proactive system must closely and reliably integrate sensors and actuators with the physical world. This task is closely related to building the infrastructure-based systems that has been described earlier. However, proactive systems will require greater sophistication in the components deployed in the environment, both to enable the capability to affect the physical world and to quickly, robustly, and accurately process real-world data. Is incomplete or imprecise knowledge of user intent still useful? At what level of uncertainty is it better to ignore such knowledge in making decisions? For example, for a building-scale temperature-monitoring application, slowly reporting distributed temperatures to a central server would be sufficient. However, an earthquake response system would need to actively dampen vibrations at many nodes throughout a building. Is the benefit worth the cost? How does one quantify this benefit?

8.4.2 Context Management

The benefits of having the universe at your fingertips are quickly overlooked if the universe is always in your face. When you are responsible for a million interaction-rich computers, these interactions are going to need to be coördinated, filtered, and exchanged, but above all mediated automatically. Users must be able to set policy for their interactions with the environment that includes the context, not only of themselves, but their interactions with other objects at any given time. Context management encompasses the mechanisms used to specify what is appropriate user interaction, and to automatically determine when and how it is appropriate. Semantic location information can be powerful for many tasks, but it remains an open problem to gather and represent both semantic position tags and detailed geometric location in a single system.

While vision has unique advantages over other sensors for tracking people, it also presents unique challenges. A person's appearance in an image varies significantly due to posture, facing direction, distance from the camera, and occlusions. It can be particularly difficult to keep track of multiple people in a room as they move around and occlude each other. Although a variety of algorithms can overcome these difficulties, the final solution must also work fast enough to make the system responsive to the room's occupants. However, as the number of connections between services increases, polling ceases to be a viable mechanism for detecting changing state. Currently, it is not possible to register event requests like "Please inform me when entity 12 intersects the extent of entity 13" or "Please inform me when CD player is finished playing". So replacing polling with an asynchronous event system is a high priority for PervComp. But again, software components are remarkably good at ignoring unwanted stimuli, but people become quickly irritated by untimely information.

8.4.3 Integration

A smart space works on the combination of information from different layers of PervComp. A seamless integration of these disparate pieces of knowledge, derived from various levels of PervNet, Pervware and applications, lead to an intelligent environment. Since the whole is much greater than the simple sum of the parts, a difficult challenge lies in the meaningful integration of component technologies, which themselves may be very simple and existing today. For example, hardware technology components include handhelds, laptops, pervasive devices, etc; network technology components include wireless communication, mobility management, etc; middleware technology components include GUI, location tracking, face recognition etc. But, real research is needed in architecture, component synthesis and system-level engineering [2].

8.4.4 System Management

A particular challenge for PervComp is the system management at the integrated level. As the number of deployed components increases, system management will likely become increasingly problematic. While the desired goal is to have zero-configuration, low-maintenance systems, the reality is that substantial system management will still likely be required. One might expect future components to support standardized management interfaces enabling, for example, tasks such as configuration management over a wide range of components. However, this management is unlikely to occur within the context of a single administrative domain. Indeed, for many components, the administrative domain might change dynamically- for example, depending on the proximity of different users or devices. The combination of requirements for low (or zero) administration, multi-domain management, and support for rapid reconfiguration will likely raise new challenges for system management.

8.4.5 Transparency

When computing moves with you, environment must have the ability to move execution state effortlessly across diverse platforms, such as desktop in the Internet, laptop and palmtop in wireless LAN, handheld in personal area networks (PANs) and so on. This personal computing space is likely to be implemented on a body-worn or handheld computer (or collection of these acting as a single PAN) known as a ''client'' of PervComp environment, even though many of its interactions may be peer-to-peer rather than strictly client-server. The client needs to be quite sophisticated and, hence, complex.

8.4.6 Thin client

A thin client is a simple terminal or other computing device connected to powerful servers where applications and data are stored and processed. The need to make pervasive devices smaller and lighter implies that their computing resources, such as processor, memory, I/O, as well as energy source (i.e., battery) have to be sacrificed. Thin pervasive devices (clients) are the next generation of computing. They are small, affordable, easy to maintain, reliable, and secure. Increasingly, enterprises are turning to thin-clients and terminal server deployments to lower their total cost of ownership (TCO). There are many reasons for this: a) less time spent upgrading software, b) standardization of desktops, c) cost savings from centralizing administration, d) increased information access across user bases, and e) often lower hardware cost. Traditionally, PC's are used as thin-clients to achieve lower TCO. In PervComp, regardless of access device, thin client mode of operation will be suitable when terminal servers have mission critical applications running on them. The stakes are raised-when the application is not available, or slow, it can affect everyone logged into the terminal server, as compared to a single end-user on a pervasive device interacting with an application. The affect on productivity, customer satisfaction, and cost can be enormous when terminal server applications do not perform to expectations.

8.4.7 Power Management

Efficient energy management requires that algorithms in the pervasive devices should be very simple, less time-consuming and very thin. But sophisticated capabilities, such as proactivity and self-tuning, increase the energy demand of software. Relentless pressure to make such devices lighter and more compact places severe restrictions on battery capacity. At the same time, they need to survive as long as possible. Rechargeable solar cells may be an alternative for devices, which are open to sunlight often. Otherwise, having longer battery life means that their computing capabilities have to be compromised. But meeting the ever-growing expectations of users may require computing and data manipulation capabilities well beyond those of a lightweight sensor, or a mobile computer with long battery life. Reconciling these contradictory requirements is another big issue. There is a growing consensus that advances in battery technology and low-power circuit design cannot, by themselves, reconcile these opposing constraints- the higher levels of the system must also be involved [2].

Now the question is how to involve the higher levels of PervComp system in energy management? In what ways can the higher levels of a system contribute to managing energy? One example is energy-aware memory management, where the operating system dynamically controls the amount of physical memory that has to be refreshed. Another example is energy-aware adaptation, where individual applications switch to modes of operation with lower fidelity and energy demand under operating system control. There can be a collaborative relationship between the operating system and applications to meet user-specified goals for battery duration. An application can dynamically modify their behavior to conserve energy. But, there remains a bunch of unanswered issues, which are critical to the approach to be followed. What are the relative strengths and weaknesses of individual approaches and when should one method be used in preference to another? How intrusive or distracting do users find such techniques? Can knowledge of user intent be exploited in energy management? If so, how robust is this approach in the face of imperfection in this knowledge? Can a system predict these savings and costs accurately enough in practice to make a significant difference?

Cyber foraging [2], construed as ''living off the land'', may be an effective way to deal with this problem. Simply speaking, cyber foraging is to use wired resource as long as possible and to shift to the nearest wired resource as quickly as possible, if it is available. For instance, when you are at home, if you receive a call in your mobile phone, the mobile phone should sense that you are near a landline phone and immediately transfer the call to it (after flashing a message on mobile phone's screen). Then, the wired telephone acts as a surrogate to the mobile phone, which saves its power at the cost of the surrogate. Many similar kinds of situations may be thought in PervComp environment. However, cyber foraging opens up many important research questions [2]. How does one discover the presence of surrogates? Does surrogate discover the presence of client or vice versa? Of the many proposed service discovery mechanisms, such as JINI, UPnP, and BlueTooth proximity detection, which is best suited for this purpose? Can one build a discovery mechanism that subsumes all of them for greatest flexibility? How secure is cyber foraging? How to transfer the service across different platforms? Is surrogate allocation based on an admission control approach, or a best-effort approach? When should one start looking for surrogates? In typical situations, how much advance notice does a surrogate need to act as an effective staging server with minimal latency? What implications does this requirement have for the other components of a pervasive computing system? What are the implications for scalability? How dense does the fixed infrastructure have to be to avoid overloads during periods of peak demand? Who will initiate the event, the client or the surrogate? What is the system support needed to make surrogate use seamless and minimally intrusive for a user?

8.4.8 Application Support

Lack of support for applications is evident from the fact that it is difficult to design, build, and deploy applications in PervComp environment. The key challenge for PervComp developers is to build applications that continue to provide useful services, even if numerous heterogeneous devices are roaming across the infrastructure and if the network provides only limited services, or none at all. Existing distributed computing technologies are ill suited to meet this challenge. Discovery services or application-aware adaptation are clearly beneficial for PervComp applications. However, they are not sufficient to successfully design, build, and deploy applications in the PervComp space. PervComp requires a common system platform, so that applications can run across (almost) all devices in this infrastructure and can be automatically distributed and installed. Heterogeneity of devices and system platforms adds more complexity to this problem. An easy solution could be a common system platform with an integrated API and a single binary format. A PervComp platform that runs across a wide range of devices does impose a least common denominator on the core APIs. Applications can only assume the services defined by the core APIs; they must implement their basic functionality within this framework. At the same time, a common platform does not prevent individual devices from exposing additional services to applications. It simply demands that additional services be treated as optional and dynamically discovered by applications.

While object-oriented programming continues to provide an attractive paradigm for application development, from the point of view of application level, objects do not scale well across large, wide-area distributed systems because of encapsulation of data and functionality within a single abstraction. This relationship between data and functionality is not applicable for PervComp. Data and functionality should be kept separate for pervasive computing applications, as they typically need to evolve independently. Also, the availability of application services is limited or intermittent in order to ensure transparency in such a highly dynamic environment. Applications need to be explicitly programmed to gracefully handle change. While this style of programming imposes a strict discipline on application developers, it also enables system services, such as check pointing and migration, previously not available in distributed systems of this scale. On the other hand, applications need to be able to acquire any resource they need at any time. These two contrasting requirements render programming and distributing applications increasingly unmanageable.

8.5 OTHER CHALLENGES

8.5.1 Economic Challenges

Today, information is the currency of new economy, and PervComp is going handle information in multiple ways. Understandably, it will be moving centre stage as success factor in the new economy. However, a common apprehension for the relative lack of success in deploying PervCom systems is that none of the application scenarios seem likely to generate significant revenue. Users might pay to live in a PervComp world, but it is difficult to imagine them paying a lot of money for any one application or feature (assuming that the search for a single "killer" application is unsuccessful). Consequently, the cost of deploying and operating a given component might need to be recovered in the form of many small contributions from PervComp applications that use the component. This will require support from components in terms of billing and accounting at a level previously unseen in widespread distributed systems. Experience design presents designers and usability specialists with a unique opportunity; but there remain a number of obstacles we need to overcome if we are to exploit it.

8.5.2 Social Challenges

In this age of information, the Internet has ushered in a new concept of user experience in handling information, leading to a free society of sharing and computing. Web users have had to contend with significant challenges to their privacy, primarily in the form of logging technologies that can generate substantial amounts of detail about a given user's Web activities. This has raised significant concerns among many Web users. PervComp is going to take it even one level more, creating a society where computing will live alongside human. Many a social barrier will fall apart in PervComp society. Commercial organizations, legislators, and privacy groups will struggle to come to terms with new technology's implications for an individual's privacy. Here lies a core problem for developers who need to create systems that better address privacy issues. Currently, users do not fully understand how the electronic trails they create can be used, so they cannot understand their personal data's value. A key challenge for future PervComp system designers is to empower users to evaluate the tradeoff between protection of privacy and access to improved service. Meanwhile, legislation must contribute by defining the boundaries within which such trade-offs may occur.

8.5.3 Legal Challenges

The Web has already demonstrated how important are the Internet Laws for its successful usage in post-deployment era. Fortunately, the Web computing has accelerated the development of legal constructs for dealing with computationally rich environments. For example, to demand that sensitive data be deleted after its use is clearly out of sync with the Internet. Most importantly, legislation must acknowledge that person-related data has become a currency in the information economy. In particular, support for adequately handling personal data challenges both legislators and PervComp systems developers. Traditionally, data protection legislation has tended to prohibit any capture and storage of person- related data and has only allowed exceptions bounded by a clearly defined purpose, at the end of which data records has to be deleted. This approach to privacy protection is inadequate for a modern, open PervComp society.

8.6 SUMMARY

For years to come, PervComp will remain a major research challenge in computer systems because practical realization of PervComp will require us to solve many difficult design and implementation issues. The first hurdle to overcome is to implement a PervNet integrating so many things that are discussed in previous chapters. Solving these problems will require us: a) to decide upon the goal in specific terms, b) to understand clearly issues involved, c) to identify the implementation priorities step-wise, d) to make use of the existing concepts, if they fit into this model, e) to broaden discourse on some topics, if needed, and finally, f) to revisit long-standing design assumptions, wherever necessary. Therefore, it is needless to say that PervComp will be the crucible in which many disjoint areas of research are to be fused.

Research challenges will include not only technical issues, but also non-technical issues, such as probable social as well as legal implications. Even technical challenges have to address issues in areas outside computer systems, such as human-computer interaction (especially multi-modal interactions and human-centric hardware designs), software agents (with specific relevance to high-level proactive behavior), and expert systems and artificial intelligence (particularly in the areas of decision making and planning) [2]. Capabilities from these areas will need to be integrated with the kinds of computer systems capabilities needed in PervComp.

REFERENCES

[1] Weiser M., "The Computer for the 21st Century", Scientific American, September, 1991.

[2] Satyanarayanan M., "Pervasive Computing: Vision and Challenges", IEEE Personal Communication, Vol. 8, No. 4, pp.10-17, Aug 2001.

[3] Special inaugural issue on *Reaching for Weiser's Vision*, IEEE Pervasive Computing, Vol. 1, No. 1, Jan-Mar 2002.

[4] Arnold D., et. al., "Discourse with Disposable Computers: How and why you will talk to your tomatoes", Proceedings of the Embedded Systems Workshop Cambridge, Massachusetts, USA, March 29–31, 1999.

Chapter 9

Vision for the Future

What distinguishes modern humankind from others is our collective ability to build more complex tools and communities. In previous eras, these amplified muscle power. In the last half century, a new kind of tool has emerged, which is known as Information Technology (IT). Its impact on society is now only dimly understood. PervComp, with its focus on users and their tasks rather than on computing devices and technology, provides an attractive vision for the future of IT. PervComp will redefine it not only by developing innovative new technologies, but also by applying expertise in human-centred systems to evaluate how well IT leverages and enhances human interaction and intellectual activity.

PervComp spreads intelligence and connectivity to more or less everything, such as ships, aircrafts, cars, bridges, tunnels, machines, refrigerators, door handles, lighting fixtures, shoes, hats, packaging. You name it, and someone, sooner or later, will put a chip in it. Whether all these chips will make for a better product, is one of the billion dollar questions. By 2005, nearly 100 million Western Europeans will be using wireless data services connected to the Internet. And that's just counting people. The number of devices using the Internet will be at least hundred times more. A vision of this kind and the associated research directions are targeted to be captured in this chapter.

9.1 HOW WE WILL WORK AND LIVE

In the past, computers were expensive. They lived in air-conditioned rooms or on desktops. More recently, we carry our own computers around with us. To gain access to the computational world, we go to a computer or take one with us, type on a keyboard or click with a mouse, and learn artificial names for the people and resources we wish to access (e.g., "ds@in.mycompany.com" or "myprinter.mynetwork.org"). The computer doesn't care, nor is it even aware, whether we are there. Virtual reality only makes matters worse: with it, we do not simply go to a computer, but also live in a reality created by a computer.

In the future, computation will be freely available everywhere, like batteries and power sockets, or water and air. Extrapolating existing trends, desktop and server systems will have greater capacity, devices will become more diverse, and information management will be better integrated. Interconnected devices will be so commonplace that "the Internet" becomes invisible. Devices span from palms (so tiny that the computer disappears) to servers (so large that storage limits vanish). Computation will enter the human world, handling our goals and needs. It will be possible to track and relate everything. We will not need to carry personalized devices around with us. Instead, "anonymous" devices, either handheld or embedded in the environment, will bring computation to us, no matter where we are or in what circumstances we are. These pervasive devices will personalize themselves in our presence by finding whatever information and software we need.

The vastness of captured information will shift the management focus from simple queries to relationships, relevance, and flow. A larger fraction of our time will be spent pushing information structuring, organizing, and storing the increasing volume within a changing environment. This will be far more expensive to administer and maintain than to build. We must wholly rethink system design: *human time and attention*, not processing or storage, are the limiting factors. Such a system will enable pervasive, human-centered interaction, not just with information, but with expertise. We will not need to type or click, nor to learn computer jargon. Instead, we will communicate naturally, using speech, vision, and phrases that describe our intent (e.g., "send this to Bob" or "get me a hardcopy quickly"), leaving it to the computer to locate appropriate resources and carry out our intent. Independent of place or time, anyone could access the combined work and collective intelligence of potentially unknown collaborators, dramatically reducing the effort to solve a problem or learn something new. This is achieved by an active system, working on behalf of the individual, gathering, accepting, filtering, aggregating, and organizing information, while protecting the owner's information assets.

In order to envision the PervComp world outlined above, starting technological assumptions are: (i) a vast diversity of computing devices (PDAs, cameras, displays, sensors, actuators, mobile robots, vehicles), (ii) "unlimited" storage (servers supporting personal storage beyond a terabyte;

anything that can be captured and stored in digital form will be), (iii) every computing device is connected roughly in proportion to its "capacity" (small devices with little bandwidth, communicating locally to larger devices with access to increased capacity), (iv) devices are predominantly "compatible," rather than predominantly incompatible (plug and play interoperation enabled by pervasive technology for on-the-fly translation, emulation, and virtual machines). The only common element is communication. Devices will be so specialized that it will be unusual to have one with an "average" amount of processor, memory, disk, display, input, and connectivity.

We have shown in this book that current technology trends are moving in this direction, but the gap is still huge to be covered as explained in the previous chapter. Our view of the future demands a quantum change in information technology research: dynamic adaptation, self-organization, and personalization on a truly massive scale. Its scale and grandeur, its rapid evolution and the radical modes of its use, the heterogeneous nature of its component subsystems and their contained information, and the broad activities it supports, make our envisioned PervComp enormously complex. We discuss some of the proposed views of PervComp model below.

9.2 DATA-CENTRIC COMPUTING

Data-centric computing is a potential revolution that could alter the way some distributed systems problems have been approached now. The main purpose is in order to make computing "invisible" to the common user, there is a need to shift the focus of technology so that human computer interactions are more task oriented and are implemented to the absolute least amount of inconvenience to the user. The fact focuses that there are many obstacles that will need to be overcome for such a vision to become a reality. Specifically, it also raises issues with the way data travels across a network, and it outlines the necessity of data objects to be able to accomplish the tasks they were appointed for without the benefit of help from the application that placed them in the network. Data items injected into the network are self-describing, may contain mobile code, and can automatically marshal resources as needed. Active data items should be able to marshal the resources they need to make progress in the network. Data moves from device to device until it reaches the service it is intended for. Mobile code fundamentally changes the assumptions about distributed systems. Whereas most systems are assumed parallel deterministic state machines, mobile code breaks this assumption and allows some nodes to perform a different set of operations based on application specific tasks and may introduce some non-determinism. Borriello [1] proposes a data-centric networking approach. He argues that even though IP now covers different physical layers and has extended to networks with mobile nodes it is not an ideal solution. Both the sender and the receiver need to be active at the same time and all the networks must be active thus tying up resources. If the data itself would become self-describing and self-directing there would be no need for a permanent connection. The data would know where its destination is. Devices could anonymously add packets to the network and thus hide their location.

To re-think the basic assumptions [2] about network operations, data-centric network architecture may be constructed as a means for distilling, naming and locating the data objects that travel within the network. Network infrastructure must be able to inform devices about the network they are using, as well as be able to provide admission control. Unlike the Internet, Bluetooth [3], HomeRF [4], USB [5], and IEEE 1394 [6] networks all reserve bandwidth for synchronous data channels. In these cases, the network infrastructure should be able to offer guarantees about the QoS to those users willing to pay a premium, provided the network has sufficient free capacity. Protocols such as RSVP and QEX [7] have only laid the initial groundwork for effective QoS management in mobile applications. Those services, which do not have specific QoS requirements, may still benefit from knowledge about the current network state. A data-centric network must also be able to manage ubiquitous persistent storage. Few existing NFS [8] offers transparent and authenticated access to a global set of files residing on a central server. Unfortunately, this system requires static configuration and has a single point of failure, making it undesirable for mobile applications. What is really needed to make this vision a reality is ubiquitous storage made available to distributed applets running across data-centric network.

9.3 UBIQUITOUS COMPUTING

When Mark Weiser coined the phrase "ubiquitous computing" in 1988 [9] he envisioned computers embedded in walls, in tabletops, and in everyday objects. In ubiquitous computing, a user might interact with hundreds of computers at a time, each invisibly embedded in the environment and wirelessly communicating with each other [10]. This can only be managed by the system implicitly organizing its contents based on tacit information extracted from the environment. Enabled by ubiquitous communication and comprehensive interoperation, implicit organization makes the utility more human-centered, by raising the level at which users interact with information. Many applications have been demonstrated in ubiquitous computing and smart environment. Some of these have concentrated on intelligent configuration of an environment based. For example, air conditioners and lights might automatically turn off when no one is in the room, or blinds may open and close depending on natural light levels in the room [11]. Other applications have implemented what is called proximate selection interfaces, where objects that are nearby are automatically easier to select. For example, a print command might automatically default to the nearest printer [12]. In a similar vein is the presentation of contextual information, where information or annotations about a particular location or object are automatically displayed to a person when she enters an area. Finally, systems have been created that watch a user's location and actions and store that information in an automatic diary [13].

The portability of ubiquitous computing devices brings additional challenges with it. Mobility is made possible through wireless communication technologies and advances in the IP protocol in the first place. There is, however, still the problem of disconnectivity. The major challenge is to automate the process of disconnection and reconnection as much as possible and the run-time should prepare for these cases without user intervention [14]. In a ubiquitous computing environment where possibly thousands and thousands of devices are part of; scalability of the whole system is a key requirement. Additionally, because all the devices are autonomous and must be able to operate independently a decentralized management will most likely be most suitable.

The simplicity is important in two major areas of every system: deployment and administration. The problem is, that most of the devices will have no dedicated administrator and no suitable administration interface. Even if the device would have an interface, the shear multitude of devices will make it virtually impossible for the owner to take on administrative responsibilities [15]. When a device gets installed initially, users should be able to just plug the device in and it should start to work immediately with no hassles [16]. In order to do so it must be able to self-configure and activate itself. And in cases of device failures or software updates, the device should be able to automatically download and install these and then to reactivate [15]. Interoperability will probably be one of the major factors for the success or failure of the Ubiquitous computing vision. It will be important that Ubiquitous computing devices and architectures can cooperatively interoperate. The system will only be successfully accepted when the easy integration of already existing technologies and devices is supported.

In a fully networked world with ubiquitous, sensor-equipped devices several privacy and security issues arise [17]. To accomplish this, the privacy and security model must be understandable by the user and it must be modelled into the system architecture [18]. Firstly, the scope of personal information must be limited. There must be ways to ensure the privacy of user locations and to determine and regulate the relationships between disjoint information systems and how they exchange personal information [19]. Secondly, there is a requirement for authentication mechanisms to ensure the identity of entities in the Ubiquitous computing environment. Then, there is the area of authorization: Who is allowed to use the system for what purpose? Finally, appropriate encryption mechanisms are required since the sea of ubiquitous devices, especially wireless-connected ones, makes the system more vulnerable to security threads.

9.4 WEARABLE COMPUTING

PervComp is not without "body computing". Pervasive means everywhere, and that include our bodies. So much so, that the boundary between human and machine is becoming blurred. However, pervasive devices that can scan, probe, penetrate and enhance our bodies have so far remained low on the radar of public awareness. Oticon, in Denmark, is developing hundred-channel amplifiers for the inner ear. Scientists are cloning body parts, in completion with engineers and designers developing replacements - artificial livers and hearts and kidneys and blood and knees and fingers and toes. And this is just to speak of stand-alone body-parts. If any of these body parts I've mentioned has a chip in it - and most of them will - that chip will most likely be connectable.

The vision behind wearable computing is that a mobile computer should not just be a machine that we put into our pocket when we plan on doing some office work while on the road. Instead it will be an integral part of our every day outfit hence wearable, always operational and equipped to assist us in dealing with a wide range of situations. They were after a new paradigm of computing - computers that would be the extension of one's personality, computers that would work with your body rather than against it, and almost needless to say, the computers that will be with you at all times, always at your disposal. In the two decades that had passed, wearable computing pioneers and the growing army of followers had had more than enough time to think through the shortcomings of their invention. Wearables are at their prime. Alongside with the new concepts in design came the new concepts in philosophy and applications.

One of the prevalent ideas in wearable computing is the concept of mediated reality. Mediated reality refers to encapsulation of the user's senses by incorporating the computer with the user's perceptive mechanisms, which are used to process the outside stimuli. For example, one can mediate their vision by applying a computer-controlled camera to enhance it. The primary activity of mediated reality is direct interaction with the computer, which means that computer is “in charge” of processing and presenting the reality to the user. A subset of mediated reality is augmented reality. It differs from the former because interaction with the computer is secondary. Just imagine a tourist arriving in a foreign city. As soon as he leaves the train his wearable computer contacts the local tourist office and compiles a list of suitable nearby hotels. It then guides the tourist towards the chosen hotel. The directions are integrated into the tourist's view of the real world using a see through computer display in his sunglasses. The display is also used to show information on landmarks and restaurants passed on the way to the hotel. At the same time the computer informs the user about any local customs or hazards that he should be aware of (e.g. ‘mind this area after dark’). Wearable computers have many applications centered on this concept of as well as many other exciting applications centered on the idea of immediate access to information. The computer must be able to operate in the background, providing enough resources to enhance but not replace the user's primary experience of reality. The wearable computing could influence on our lives as profoundly as the emergence of the PC and the Internet. However before this happens wearable systems must overcome a number of shortcomings that currently make them unsuitable for widespread use. This has motivated many academic and industrial wearable-computing projects recently [20].

A wearable computer is often described as a system that is [21]

- unobtrusive to the point of being an integral part of the users clothing,
- portable while operational and always on,
- equipped with a hands free or nearly hands free user interface,
- able to augment the users perception of the reality e.g. merge a computer generated image with the users view of the world using a see through display,
- context and environment sensing knows what the user does and what is happening around him/her and
- able to act on the users behalf even without his/her knowledge and get his/her attention whenever required

The above properties enable the wearable computer to assist humans in tasks involving, intensive, real time interaction with the environment. Such tasks arise in equipment maintenance, search and rescue operations, surgery, security surveillance, education as well as leisure activities like golf or skiing. The system can provide the user with assistance in three general areas: (1) extended perception through an array of sensors and signal processors, (2) communication capabilities and (3) real time access to databases and computing power. The main issues on the way to a truly wearable computer are:

- adequate miniaturized input devices,
- unobtrusive, see through displays with high resolution and low power consumption,
- a user interface that is adequate for augmented reality wearable applications,
- compact, low power computer systems capable of dealing with the high signal processing and graphics load encountered in wearable computing,
- miniaturized sensors,
- a cableless network technology for the interconnection of the wearable components distributed over the users body (body area network)

The above problems pose engineering and scientific challenges in five broad areas: (1) the miniaturization of complex electro-opto-mechanical systems, (2) high performance electronic devices and packaging, (3) computer architecture, (4) object tracking and image recognition, and (5) human computer interfaces. All of the above areas are rapidly advancing to open up possibilities for improvements in wearable technology.

9.5 DISPOSABLE COMPUTING

Beyond ubiquitous computing, is the advent of disposable computing, occurring when the price of an embedded computer becomes insignificant compared to the cost of goods [22]. While the availability of ubiquitously “wired” goods is currently a novelty, it will soon be not only commonplace, but all pervasive. While it is easy to imagine networked toasters, fridges, televisions, and indeed, any already electronic device, following these will be the second wave of wired devices; the era of *disposable computing*, when the price of embedding a computer becomes insignificant compared to the cost of manufacture. Far more than ubiquitous computing, disposable computing will wreak fundamental changes in the nature of computing, allowing almost every object encountered in daily life to be “aware”, to interact, and to exist in both the physical and virtual worlds. In particular, disposable computing dictates a new approach to interaction amongst software components, and between software and human users. The issue facing software architects is how do we effectively use networked food, clothing, paper, books, people, doors, cars and roads? What communication strategies are needed?

When you throw you lunch wrapper in the trash, its computer negotiates with the trashcan to be recycled or shredded or composted. But your lunch wrapper was bought using your debit account, and the trashcan wants to charge you for burdening it with non-recyclable plastic. The possibility for eavesdropping and losing sensitive information becomes overwhelming once computers are disposable. The volume of data available about you and your life becomes absolutely staggering. How do we secure your information environment whilst retaining the availability and mobility of your data? How do we balance the benefits of availability whilst protecting against intrusion. But the universe of disposable computing is populated with devices whose type and identity are completely unknown to the other devices they will have to interact with. The continual churn of devices relevant to a task will completely overwhelm the current solutions of name servers and addresses within the homogeneous IP network. Disposable computing requires a revolution in distributed systems; existing paradigms will not scale effectively to support the rapidly changing environment of vast numbers of relevant objects.

9.6 SMART ENVIRONMENT

Our houses are going the same way, crammed full of chips and sensors and actuators and god knows what. And to judge by this picture, increasingly bloated and hideous. Imagine the scenario: You are driving home from work and your cell phone rings. “Your refrigerator is on the line”, the car says; “it wants you to pick up some milk on your way home”. Why is it that all these “house of the future” designs are so ghastly? Increasingly, many of the chips around us will sense their environment in rudimentary but effective ways. The world is already filled with eight, twelve, or thirty computer chips for every man, woman and child on the planet. The number depends on whom you ask, within a few years - say, the amount of time a child who is four years old today will spend in junior school - that number will rise to thousands of chips per person. A majority of these chips will have the capacity to communicate with each other.

The smart home offers a new opportunity to augment people's lives with PervComp technology that provides increased communications, awareness, and functionality. A smart environment is based on a physical environment such as a house (e.g., the Aware Home [24]) or room (e.g., the iRoom [25]) equipped with sensors and actuators. What makes the environment smart is that services and applications in the infrastructure process the sensor readings, in order to trigger events, to adapt their behaviour or to control the physical state of the room. The Aware Home has ‘smart floors’ to recognise the occupants from their footsteps. This and other sensing techniques are used in applications such as helping users find lost objects. In the Aware Home [24], services and applications persist in the infrastructure while the physical contents change. An interesting variation is where the virtual contents also change as humans and other physical contents come and go. Recently, a number of trends have increased the likelihood that the aware home can soon become a reality. Trends such as Moore's Law, the proliferation of networkable devices, wireless technologies, and an increasing vendor focus on technologies for the home are driving awareness of the smart home idea out of academia and into mainstream thinking [26] [27]. A number of challenges from the technical, social, and pragmatic domains must be overcome before the vision of the smart home can become a reality [28]. These challenges arise from the ways in which users expect smart homes to be deployed and inhabited; technical questions of interoperability, manageability, and reliability; social concerns about the adoption of domestic technologies and the implications of such technologies; and design issues that arise from considering just how smart the smart home must be.

There are a number of problems that arise that are unique to the smart home setting itself. Existing houses were not designed to be smart, and office technologies are often intended to be just those technologies for the office rather than the home. There are hosts of technical, implementation, and systems design issues. Further, the *tradeoffs* among these issues are not well understood in the home setting. The stringent requirements for reliability, the fact that there will be no formal systems administrator (nor will most home owners be likely to want to undertake such a role), and the desire for interoperability all trade off against each other.

The social impact of new technologies is hard to predict. The home setting is not novel in this respect, although the social dynamics and relationships within the home make it perhaps a more volatile setting than the office or other public spaces. Finally, the philosophical question that should be addressed by designers of smart home technology is, simply, how smart does the smart home have to be to provide utility to its occupant-owners? To some degree, this question permeates all of the others issues raised, since it is precisely the "smartness" of the smart home that makes it disruptive to the domestic order, gives rise to the architectural and implementation tradeoffs mentioned above. The chief challenge that will be faced by the designers and, potentially, the occupants of the smart home is balancing the desire for innovative technological capabilities with the desire for a domestic lifestyle that is easy, calming, and- at least in terms of technology- predictable.

9.7 EPILOGUE

What happens to our present society when there are hundreds of microchips for every man, woman and every living object? What cultural consequences follow when every object around us is 'smart', and connected? And what happens psychologically when you step into the garden to look at the flowers- and the flowers look at you? We know how to do amazing things, and we're filling the world up with amazing systems and devices. But we cannot answer the question: what is this stuff for? What value does it add to our lives? The dilemma is that we are increasingly at a loss to understand what to make. We have landed ourselves with an industrial system that is brilliant on means, but pretty hopeless when it comes to ends. We can deliver amazing performance, but we find value hard to think about.

It's not so much that technology is changing quickly- change is one of the constants we have become used to. And it is not that technology is penetrating every aspect of our lives: that, too, has been happening to all of us since we were born. It is the rate of acceleration of change that is alarming. Think of it as a combination of Moore's Law (which states that processor speeds double and costs halve every 18 months or so) and Metcalfe's Law (which states that the value of a network rises in proportion to the number of people attached to it).

REFERENCES

[1] Borriello G. The Challenges to Invisible Computing. IEEE Computer 2000; 123-125

[2] Esler M., Hightower J., Anderson J., Borriello G. Next century challenges: data centric networking for mobile computing, The Portolano Project at the Univ of Washington. Proceedings Mobicom 1999; Seattle, Washington

[3] Bluetooth SIG. Bluetooth technology 1999; http:// www.bluetooth.com/technology

[4] HomeRF working group. HomeRF 1999; www.homerf.org

[5] Universal serial bus specification revision 1.1. Technical report, Compaq, Intel, Microsoft & NEC 1988; www.usb.org/developers/data/usb11.pdf

[6] Kunzman A.J, Wetzel A.T. 1394 high performance serial bus: the digital interface for ATV. IEEE Trans on Consumers Electronics 1995; 893-900

[7] Davis N., et.al. Distributed systems support for adaptive mobile applications. Mobile Networks and Applications 1996; 399-408

[8] SUN Microsystems. The NFS distributed file system. Technical report 1995; Palo Alto, CA

[9] Rhodes J B., Minar N, Weaver J. Wearable computing meets ubiquitous computing. Proceedings ISWC 1999; San Francisco, CA

[10] Weiser M. Some computer science problems in ubiquitous computing. Communications of the ACM 1999; 74-83

[11] Elord S., et.al. Responsive office environments. Communications of the ACM 1993

[12] Schilit B., Adams N., Want R. Context-ware commuting applications. Workshop on Mobile Computing Systems & Applications 1994; Santa Cruz, CA

[13] Lamming M., et.al. The design of a human memory prosthesis. The Computer Journal 1994; 153-63

[14] Banavar G., et.al. Challenges: An application model for pervasive computing. Proceedings 6th Annual International Conference on Mobile Computing & Networking 2000

[15] Andersson J. A deployment system for pervasive computing. Proceeding International Conference on Software Engineering 2000

[16] Larsson., Christensson B. Universal plug & play connects smart devices. WinHEC 99 white paper 2001; Axis Communications Inc.

[17] Press L. Personal computing: The past PC era. Communications of the ACM 1999; 21-24

[18] Schmidt A., Beigel M. New challenges of ubiquitous computing & augmented reality. Proceedings 5th CaberNet Radicals Workshop 1998

[19] Russell D M., Weiser. The future of integrated design of ubiquitous computing in combined real and virtual worlds. Proceedings Conference on Human Factors in Computing Science 1998

[20] Wearable Computing laboratory. The vision and reality of wearable computing. www.ife.ee.ethz.ch

[21] Billinghorst M. Wearable computers: Beyond handheld computing. Tutorial 1st International Symposium on Handheld and Ubiquitous Computing 1999; Karlsruhe

[22] Arnold D., et.al. Discourse with disposable computers: how and why you will talk to your tomatoes. www.dstc.edu.au 1999

[23] Weiser Mark. The computer for the 21st century. Scientific American 1991

[24] Kidd C. et.al. The aware home: a living laboratory for ubiquitous computing research. Proc 2nd International Workshop on Cooperative Buildings-CoBuild 1999

[25] Fox A., et.al. Integrating information appliances into an interactive workspace. IEEE Computer Graphic and Application 2000

[26] Buderi R. Computing goes everywhere. Technology Review 2001; 53-59

[27] Hales L. Blops, Pods & People. The Wall Street Journal Mar 25 2001

[28] Edwards K W., Grinter R.E. At home with ubiquitous computing: seven challenges. Proceedings Ubicomp 2001; Berlin Heidlberg.

Index